Clare Controls IP Network Cameras User Guide

Last Modified: 14 October, 2015

Note: The Clare Controls IP Network Cameras User Guide will no longer be updated. For up to date IP Network Cameras, see our Knowledge Base.

https://knowledgebaseclarecontrols.atlassian.net/wiki/display/CVIS/Clare+Controls+IP+Network+Cameras+User+Guide

Doc ID - 343 • Rev 05

Copyright © 14OCT15 Clare Controls, Inc. All rights reserved.

This document may not be copied in whole or in part or otherwise reproduced without prior written consent from Clare Controls, Inc., except where specifically permitted under US and international copyright law.

Trademarks and patents The Clare Controls IP Network Cameras name and logo are trademarks of Clare Controls, Inc.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Version This document applies to Clare Controls IP Network Cameras version 01.

FCC compliance This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC compliance This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his or her own expense.

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EC.

2002/96/EC (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Contact information For contact information, see www.clarecontrols.com.

Disclaimer statement

“Underwriters Laboratories Inc. (“UL”) has not tested the performance or reliability of the security or signaling aspects of this product. UL has only tested for fire, shock or casualty hazards as outlined in UL’s Standard(s) for Safety, UL60950-1. UL Certification does not cover the performance or reliability of the security or signaling aspects of this product. UL MAKES NO REPRESENTATIONS, WARRANTIES OR CERTIFICATIONS WHATSOEVER REGARDING THE PERFORMANCE OR RELIABILITY OF ANY SECURITY OR SIGNALING RELATED FUNCTIONS OF THIS PRODUCT.”

Content

Important information...1
Limitation of liability...1
Safety warnings and cautions...2
Advisory messages...3
System requirement...4

Network connection...5
Setting the network camera over a LAN...5
Wiring over a LAN...5
Detecting and changing the IP address...6
Setting the network camera over a WAN...7
Static IP connection...7
Connecting the network camera with static IP directly...7
Dynamic IP connection...8
Connecting the network camera via a modem...8

Access to the network camera...10
Accessing by web browsers...10

Wi-Fi settings...13
Configuring Wi-Fi connection in manage and ad-hoc modes...13
Wireless connection in ad-hoc mode...14
Security mode...15
WPA-personal and WPA2-personal mode:...16
WPA- enterprise and WPA2-enterprise mode:...16
Easy Wi-Fi connection with WPS function...17
PBC mode:...18
PIN mode:...18
IP property settings for wireless network connection...20

Live View...21
Live View page...21
Starting live view...22
Full-screen mode...22
Recording and capturing pictures manually...22
Operating PTZ control...53
PTZ control panel...53
Setting/calling a preset...61
Configuring Live View parameters...23

Network camera configuration...24
Configuring local parameters...24
Configuring time settings...25
Configuring TCP/IP settings...27
Configuring port settings...28
Configuring PPPoE settings...28
Configuring DDNS settings...29
Configuring SNMP settings...31
Configuring 802.1X settings...32
Configuring QoS settings...33
Configuring FTP settings...33
Configuring UPnP settings...34
Configuring video settings...35
Configuring audio settings...37
Configuring ROI encoding...38
Configuring image parameters...38
Configuring display settings...38
Configuring OSD Settings...41
Configuring text overlay settings...42
Configuring privacy mask...43
Configuring picture overlay...44
Configuring and handling alarms...45
Configuring motion detection...45
Arming schedule for motion detection...46
Set the alarm actions for motion detection....47
Configuring video tampering alarm...47
Handling exception...48
Email sending triggered by alarm...49
Configuring snapshot settings...50
Uploading to FTP...50
Configuring other alarms...51

Configuring PTZ...53
Configuring the basic PTZ settings...53
Configuring the PTZ limit settings...55
Configuring the initial PTZ position...56
Configuring the PTZ park action...57
Configuring the PTZ privacy mask...57
Configuring a PTZ scheduled task...58
Clearing a PTZ configuration...60
Configuring the prioritize PTZ...60

Storage settings...61
Configuring NAS settings...62
Configuring recording schedule...63

Playback...67

Log searching...69

Others...70
Understanding camera capacity in an NVR...70
    Streaming video types...70
    Adjusting settings...71
Managing user accounts...71
Configuring RTSP authentication...73
Anonymous visit...73
IP address filter...74
Viewing device information...76
Maintenance...76
Rebooting the camera...76
Restoring default settings...77
Importing/exporting configuration files...77
Upgrading the system...78
RS-232 settings...78
RS-485 settings...79

Appendix 1...80
SADP software introduction...80
    Description of SADP V 2.0...80
    Search online devices manually...81
    Modify network parameters...81

Appendix 2...82
Port mapping...82

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will Clare Controls, Inc. be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of Clare Controls, Inc. shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether Clare Controls, Inc. has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, Clare Controls, Inc. assumes no responsibility for errors or omissions.

Safety warnings and cautions

Please pay attention to the following warnings and cautions.

Hazardous voltage may be present: Special measures and precautions must be taken when using this device. Some voltages on the device may present a hazard to the user. This device should only be used by employees from our company with knowledge and training in working with devices that contain live circuits.

Caution
The power supply in this product contains no user-serviceable parts. Refer servicing only to qualified personel.

Power supply hazardous voltage: AC mains voltages are present within the power supply assembly. This device must be connected to a UL approved, completely enclosed power supply, of the proper rated voltage and current. There are no user serviceable parts inside the power supply.

WARNING
RISK OF ELECTRIC SHOCK
Connect only to a properly earth grounded outlet.
Apparaten skall anslutas till jordat uttag när den ansluts till ett nätverk.

System grounding (Earthing): To avoid shock, ensure that no AC wiring is exposed and that the earth grounding is maintained. Ensure that any equipment to which this device will be attached is also connected properly to wired, grounded receptacles.

Power connect and disconnect: The AC power supply cord is the main disconnect device to mains (AC power). The socket outlet should to be installed near the equipment and be easily accessible.

Installation and Maintenance: Do not connect/disconnect any cables or perform installation/maintenance on this device during an electrical storm.

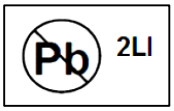
Power cord requirements: The connector that plugs into the wall outlet must be a grounding-type male plug designed for use in your region. It must have certification by an agency in your region. The connector that plugs into the AC receptacle on the power supply must be an IEC 320, sheet C13, female connector. See the following website for more information http://kropla.com/electric2.htm.

Lithium battery: This device contains a lithium battery. There is an explosion risk if the battery is replaced with an incorrect type. Dispose of the used batteries according to the vendor's instructions and in accordance with local environmental regulations.

Perchlorate material: Special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate. This notice is required by California Code of Regulations, Title 22, Division 4.5, and Chapter 33: Best Management Practices for Perchlorate Materials. This device includes a battery which contains perchlorate material.

Thermal and mechanical injury: Some components such as heat sinks, power regulators, and processors may be hot. Care should be taken to avoid contact with these components.

Electromagnetic interference: This equipment has not been tested for compliance with emission limits of the FCC and similar international regulations. This device is not, and may not be, offered for sale or lease without authorization from the United States FCC or its equivalent in other countries. It is prohibited to use this equipment in a residential location. This equipment generates, uses, and can radiate radio frequency energy. This can result in harmful interference to radio communications.



Lead content: Recycle this device in a responsible manner. Refer to local environmental regulations for proper recycling; do not dispose of device in unsorted municipal waste.

Advisory messages

Warnings

- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 24 VAC or 12 VDC according to the IEC60950-1 standard.
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Install blackout equipment in the power supply circuit for convenient supply interruption.
- Make sure that the ceiling can support more than 50 (N) Newton gravities.
- Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Cautions

- Before using the camera, make sure the power supply voltage is correct.
- Do not drop or subject the camera to physical shock.
- Do not touch the sensor modules with your fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period, put the lens cap on to protect the sensor from dirt.
- Do not aim the camera lens at strong light such as the sun or an incandescent lamp. This can cause severe damage to the camera.
- The sensor may be burned out by a laser beam. Make sure that the surface of the sensor is not exposed to laser equipment.
- Do not place the camera in extremely hot or cold temperatures (the operating temperature should be between 14 to 140˚F (-10 to 60°C) or in dusty or damp environments.
- Good ventilation is required for a proper operating environment avoiding heat accumulation.
- Keep away from water or any liquid.
- When returning, the camera should be in its original packing.
- Improper use or replacement of the battery may result in explosion. Always use the manufacturer recommended battery type.

System requirement

Operating system: Microsoft Windows XP SP1 and above version / Vista / Win7 / Server 2003 / Server 2008 32 bits

CPU: Intel Pentium IV 3.0 GHz, or higher

RAM: 1 G or higher

Display: 1024 × 768 resolution, or higher

Web browser: Internet Explorer 6.0, and above; Apple Safari 5.02, and above; Mozilla Firefox 3.5, and above; and Google Chrome 8, and above.

Network connection

If you want to set the network camera via a LAN (Local Area Network), refer to “Setting the network camera over a LAN” on page 5.

If you want to set the network camera via a WAN (Wide Area Network), refer to “Setting the network camera over a WAN” on page 7.

Setting the network camera over a LAN

To view and configure the camera via LAN, you must connect the network camera in the same subnet as your computer. Install the SADP software to search for and change the IP of the network camera.

Note: For the detailed introduction of SADP, refer to Appendix 1.

Wiring over a LAN

The following figures show the two ways for establishing the cable connection of a network camera and a computer.

To test the network camera, connect it directly to the computer with a network cable, as shown in Figure 1.

Refer to Figure 2 to set the network camera over a LAN, via a switch or using a router.

Figure 1: Connecting directly

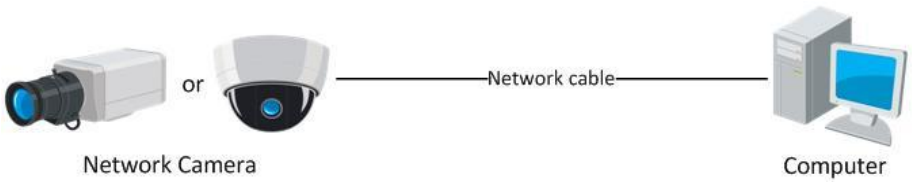
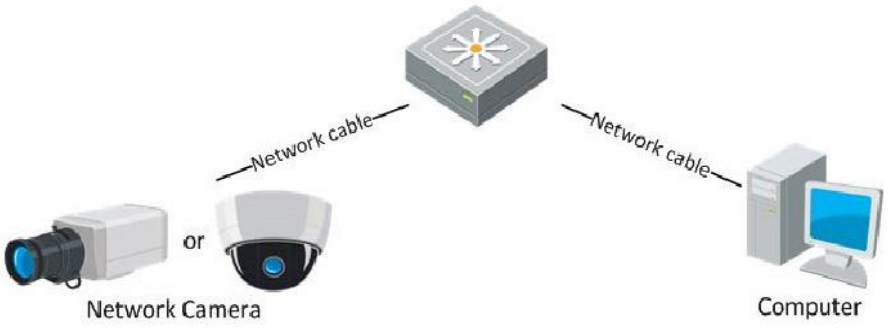


Figure 2: Connecting via a switch or a router



Detecting and changing the IP address

You need the IP address to visit the network camera.

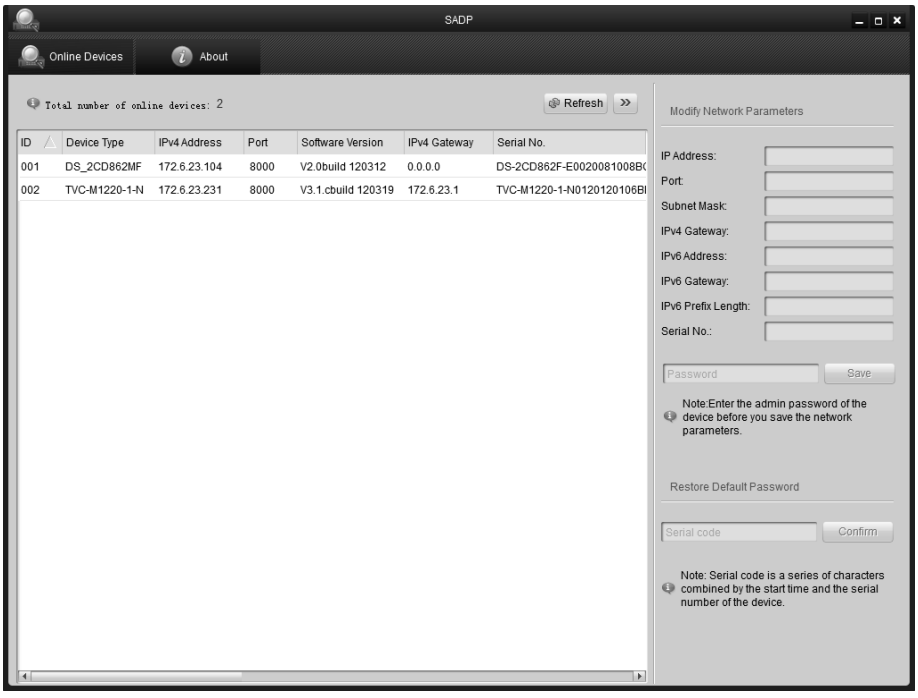
To detect and change the IP address:

1. To get the IP address, you can choose one of the following methods:
   - Use SADP, a software tool which can automatically detect the online network cameras in a LAN. List the device information including IP address, subnet mask, port number, device serial number, device version, etc., shown in Figure 3.
   - Use the client software to list all online devices. Refer to the user manual or client software for detailed information.
2. Change the IP address and subnet mask to match your computer.
3. Enter the IP address of the network camera in the address field of the web browser to view the live video.

Notes

- The default IP address is 192.168.1.250 and the port number is 8000. The default user name is clareadmin, and password is secure7.
- For accessing the network camera from different subnets, set the gateway for the network camera after you have logged in.

Figure 3: SADP interface



Setting the network camera over a WAN

This section explains how to connect the network camera to a WAN with a static IP or a dynamic IP.

Static IP connection

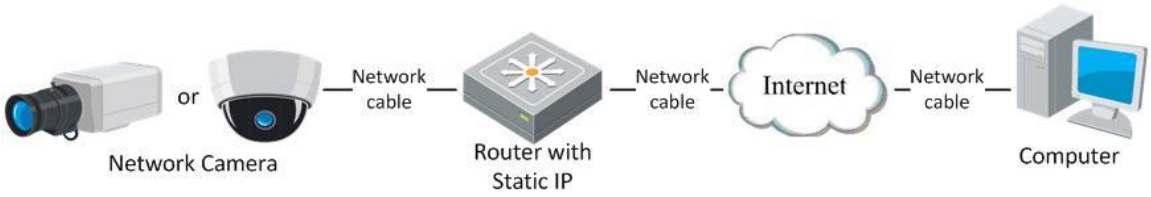
Apply a static IP from an ISP (Internet Service Provider). With the static IP address, you can connect the network camera via a router or connect it to a WAN directly.

To connect the network camera via a router:

1. Connect the network camera to the router.
2. Assign the LAN IP address, subnet mask, and gateway.
3. Save the static IP in the router.
4. Set port mapping – for example, 80, 8000, 8200, and the 554 ports. The steps for port mapping vary based on router. Call the router manufacturer for assistance with port mapping.

   Note: Refer to Appendix 2 for detailed information about port mapping.
5. Visit the network camera through a web browser or the client software.

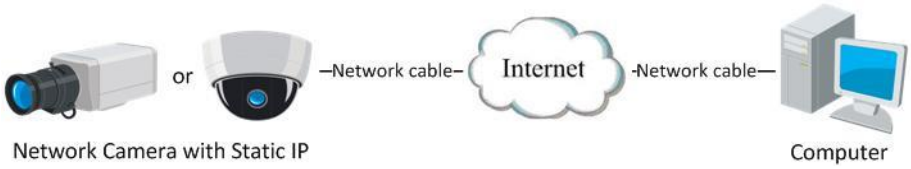
Figure 4: Accessing the camera though a router with a static IP



Connecting the network camera with static IP directly

You can save the static IP in the camera and connect it directly to the internet without using a router.

Figure 5: Accessing the camera with static IP directly



Dynamic IP connection

Apply a dynamic IP from an ISP. With the dynamic IP address, you can connect the network camera to a modem or a router.

To connect the network camera via a router

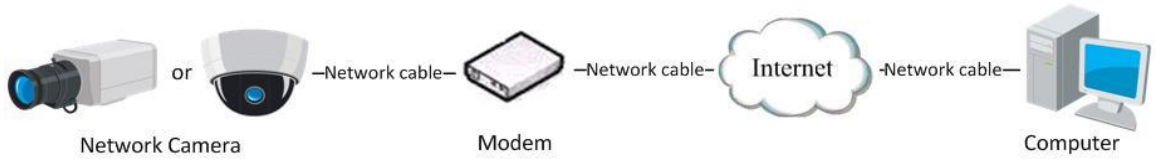
1. Connect the network camera to the router.
2. In the camera, assign a LAN IP address, subnet mask, and gateway.
3. In the router, set the PPPoE user name and password.
4. Set port mapping, e.g., 80, 8000, 8200 and the 554 ports. The steps for port mapping vary based on router. Call the router manufacturer for assistance with port mapping.

   Note: Refer to Appendix 2 for detailed information about port mapping.
5. Apply a domain name from a domain name provider.
6. Configure the DDNS settings in the setting interface of the router.
7. Visit the camera via the applied domain name.

Connecting the network camera via a modem

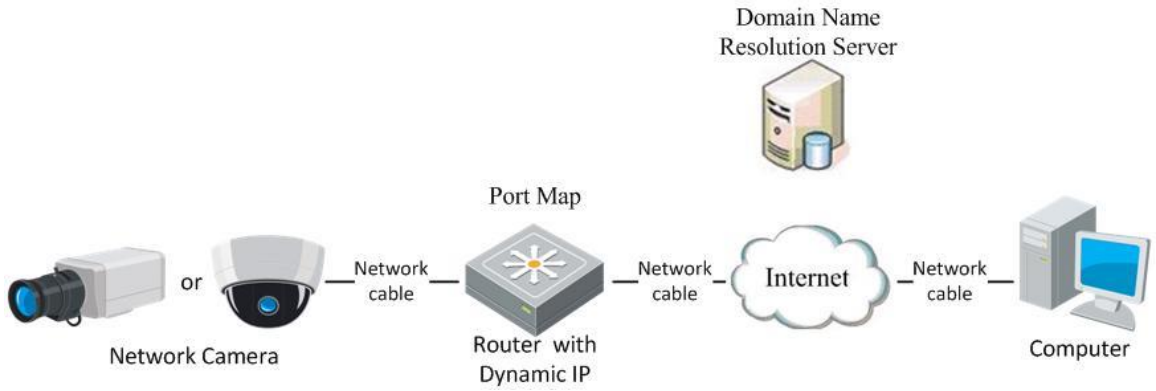
If the camera supports the PPPoE auto dial-up function, the camera receives a public IP address. This is done by ADSL dial-up, after the camera is connected to a modem. Configure the PPPoE parameters of the network camera.

Figure 6: Accessing the camera with dynamic IP



Note: The obtained IP address is dynamically assigned via PPPoE, so the IP address will change after every reboot. To stop this from happening, obtain a domain name from a DDNS provider – for example, www.myclarevision.com. Follow the below steps for normal and private domain name resolution.

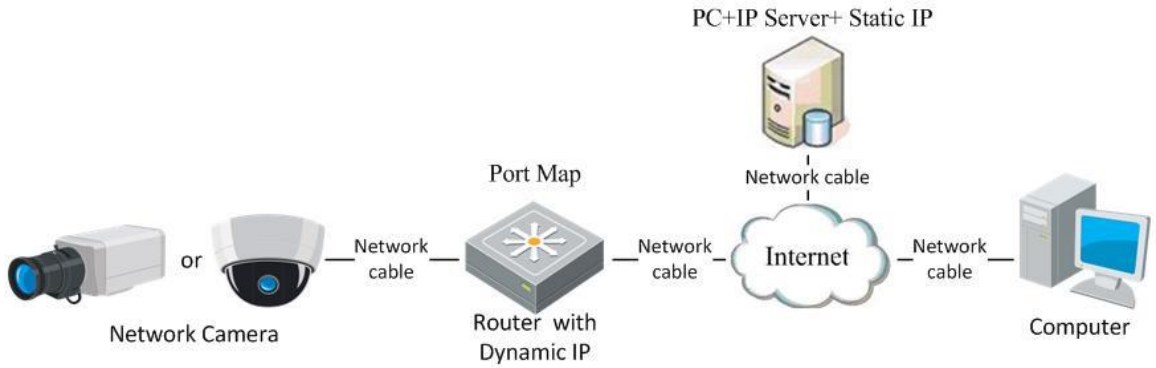
Figure 7: Normal domain name resolution



Steps:

1. Obtain and apply a domain name from a domain name provider.
2. Configure the DDNS settings in the DDNS settings interface of the network camera, and then click **Save**.
3. When prompted, reboot for the settings to take effect.
4. Configure the DDNS settings of the camera via the applied domain name.

Figure 8: Private domain name resolution



Steps:

1. Install and run the IP server software on a computer with a static IP.
2. Access the network camera through a LAN with a web browser or the client software.
3. Enable DDNS and select the IP Server as the protocol type, and then click **Save**.
4. When prompted, reboot for the settings to take effect.

Access to the network camera

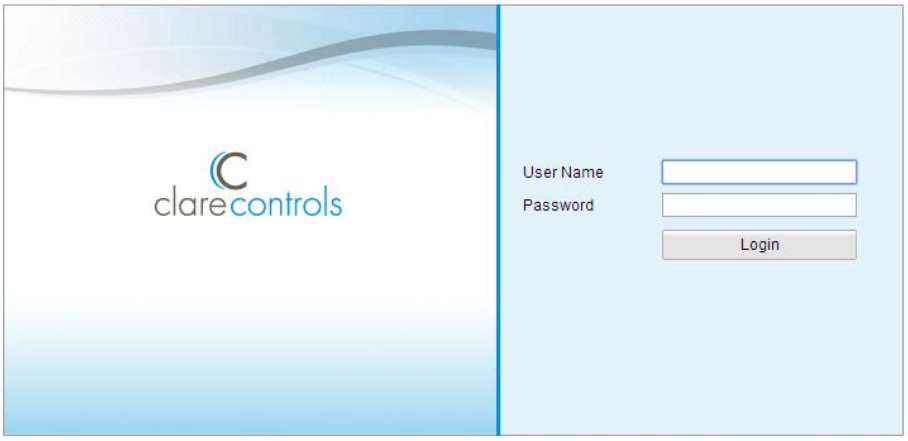
Accessing by web browsers

Accessing the network camera through a web browser lets you view the camera feed and configure the cameras settings.

To access the camera by web browsers:

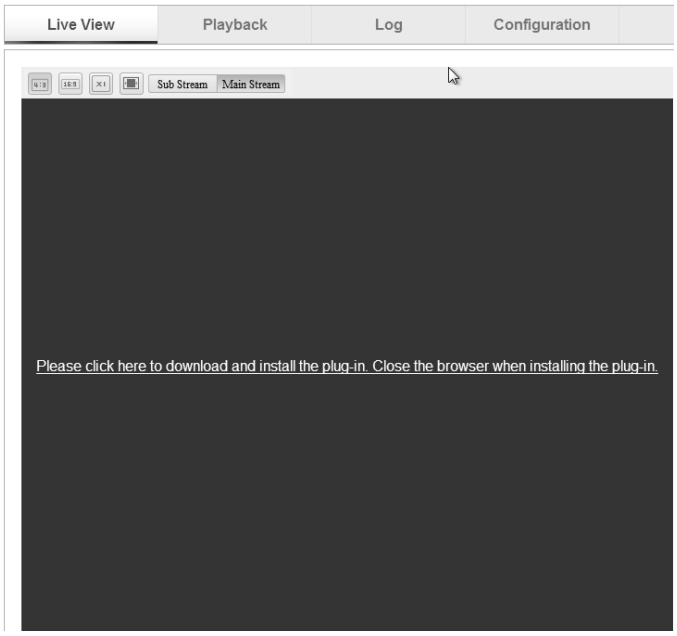
1. Open the web browser.
2. In the address field, enter the IP address of the network camera (e.g., 192.168.1.250), and then press **Enter**.
   This brings you to the login interface.
3. Enter the user name and password, and then click **Login**.

   Note: The default user name is clareadmin and the password is secure7

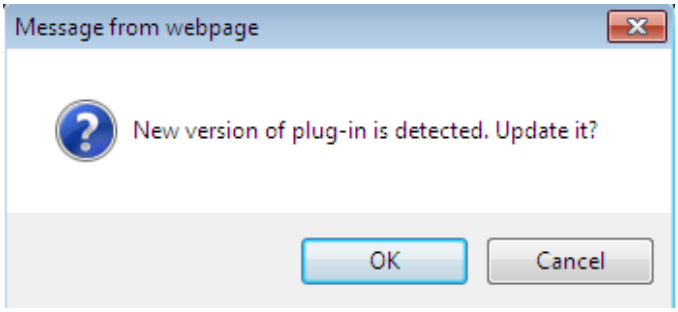


4. Install the plug-in, if prompted, and follow the installation prompts before viewing the live video and operating the camera.

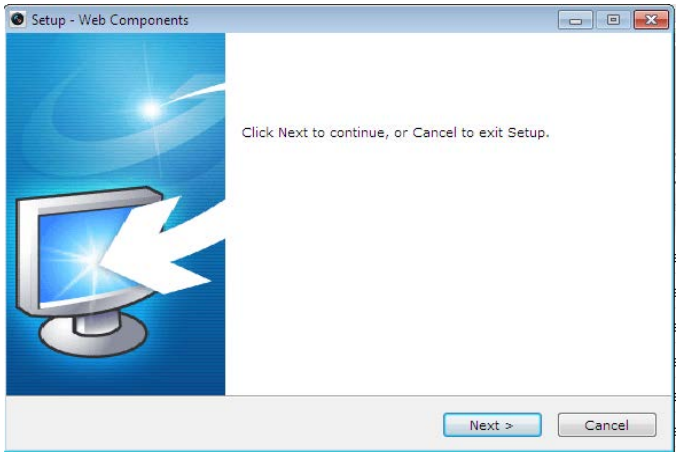
   Note: You may need to close the web browser to install the plug-in. After installing the plug-in, reopen the web browser and log in.



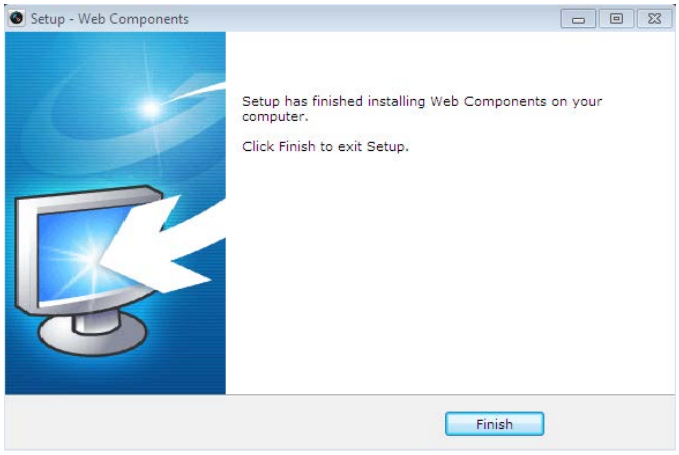
5. Click **OK**.



6. Click **Next**.



7. Click **Finish**.



Wi-Fi settings

You do not need to use cables when connecting to the wireless network.

Note: This chapter is only applicable for the cameras with a Wi-Fi module built-in, like the Clare Controls 1.3 MP Budget Mini-Dome Camera with Wi-Fi.

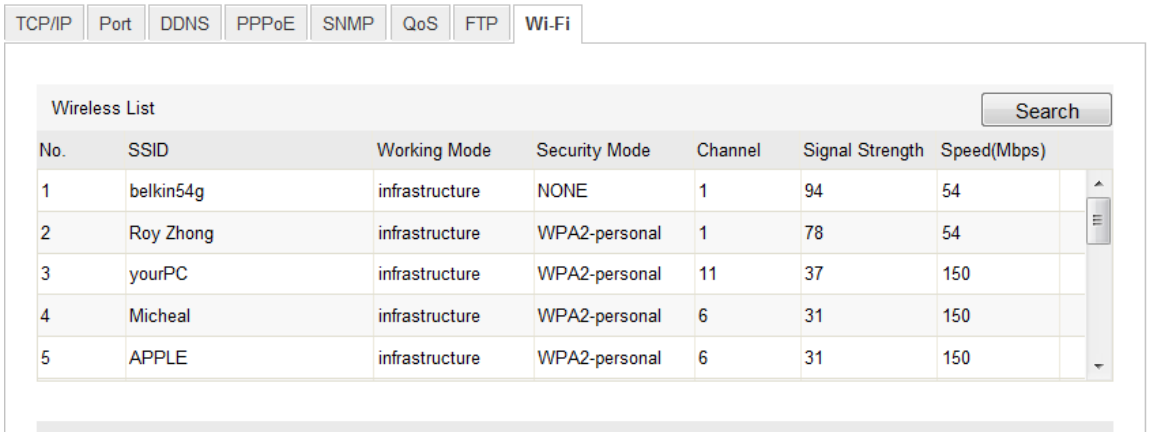
Configuring Wi-Fi connection in manage and ad-hoc modes

A wireless network must be configured.

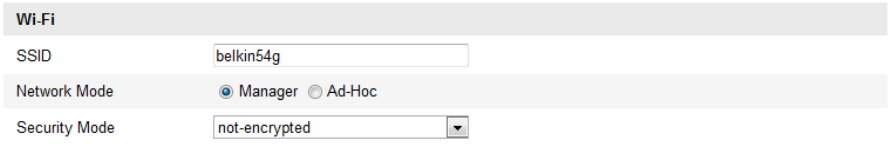
To configure a wireless connection in Manage Mode:

1. Enter the Wi-Fi configuration interface.

   Configuration > Camera Configuration > Network > Wi-Fi



2. Click Search to search the online wireless connections.
3. Click to select a wireless connection on the list.



4. Set the Network Mode to Manager.
5. The Security Mode and the network Encryption Type are automatically selected when you choose the wireless network, do not change it manually.

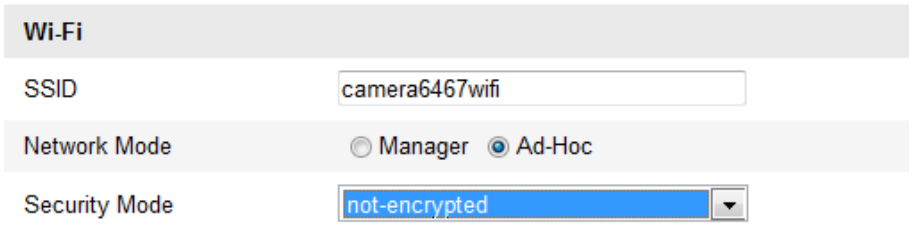
   Note: These parameters must match the router.
6. Enter the password to connect the wireless network. The password should be that of the wireless network connection you set on the router.

Wireless connection in ad-hoc mode

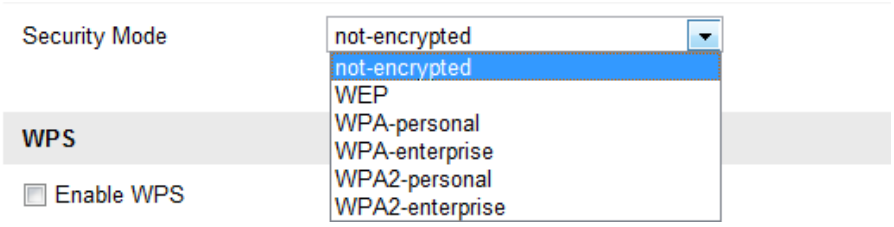
If you choose Ad-Hoc mode, you do not need to connect the wireless camera via a router. The camera broadcast the wireless signal. Connect the camera directly to the PC with a network cable.

To configure a wireless connection in ad-hoc mode:

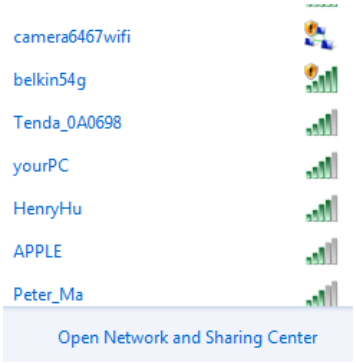
1. Choose Ad-Hoc mode.



2. Customize the SSID for the camera.
3. Choose the Security Mode of the wireless connection.



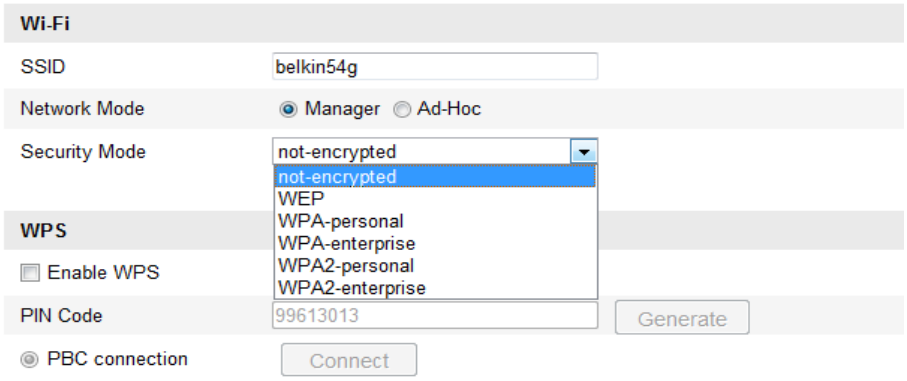
4. Enable the wireless connection function for your PC.
5. On the PC, search the network to see see the SSID of the camera listed.



6. Choose the SSID and connect.

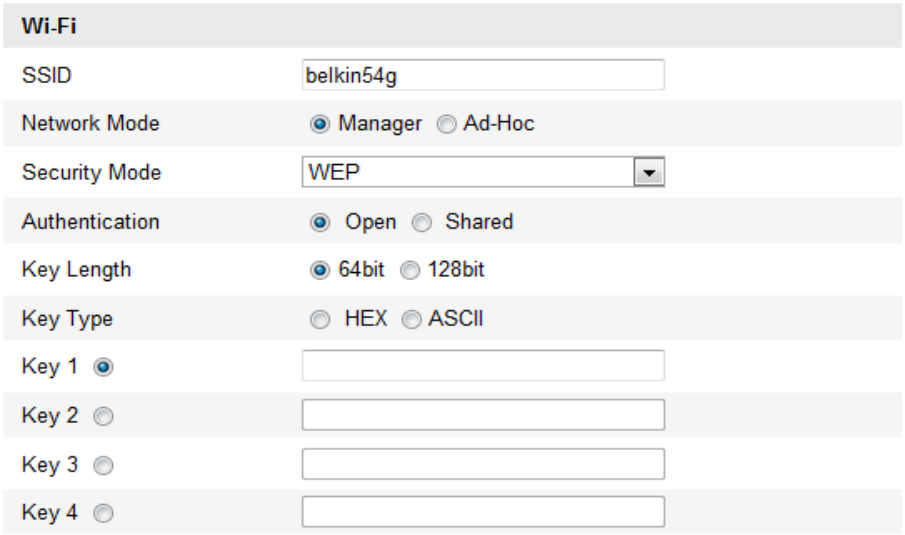
Security mode

Figure 9: Security Mode Options



You select the Security Mode; not-encrypted, WEP, WPA-personal, WPA-enterprise, WPA2-personal, and WPA2-enterprise.

Figure 10: WEP Mode

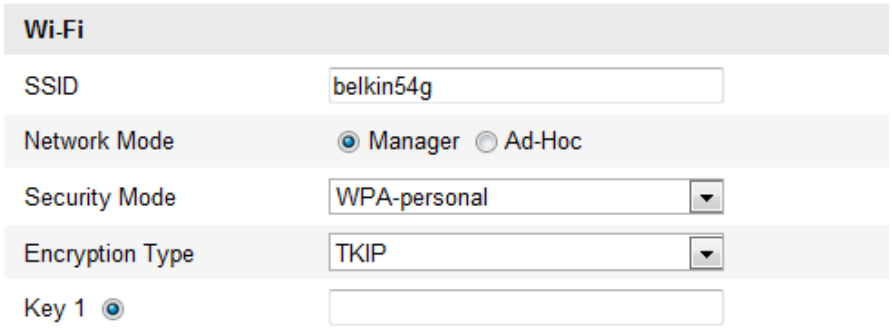


- **Authentication** - Select Open or Shared Key System Authentication, depending on the method used by the access point. Not all access points have this option.
- **Key Length** - This sets the length of the key used for the wireless encryption, 64 or 128 bit. The encryption key length can sometimes be shown as 40/64 and 104/128.
- **Key Type** - The key types depend on the access point being used. The following options are available:
  - HEX - Allows you to manually enter the hex key.
  - ASCII - In this method the string must be exactly 5 characters for 64 bit WEP and 13 characters for 128 bit WEP.

WPA-personal and WPA2-personal mode:

Enter the required pre-shared key for the access point, a hexadecimal number or a passphrase.

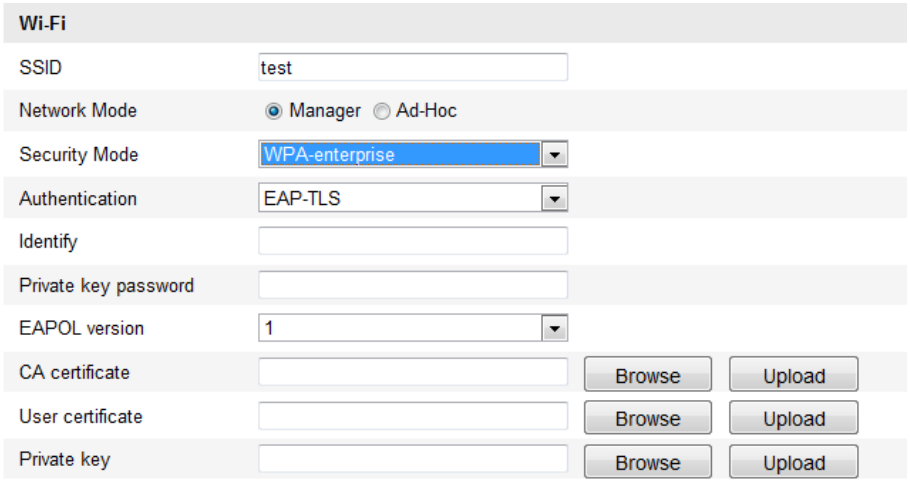
Figure 11: Wi-Fi key 1



WPA- enterprise and WPA2-enterprise mode:

Choose the type of client/server authentication being used by the access point: EAP-TLS or EAP-PEAP.

Figure 12: EAP-TLS



EAP-TLS

- **Identity** - Enter the user ID to present to the network.
- **Private key password** – Enter the password for your user ID.
- **EAPOL version** - Select the version used (1 or 2) in your access point.
- **CA certificates** - Upload a CA certificate to present to the access point for authentication.

EAP-PEAP:

- **User Name** - Enter the user name to present to the network.
- **Password** - Enter the password of the network.
- **PEAP Version** - Select the PEAP version used at the access point.
- **Label** - Select the label used by the access point.
- **EAPOL version** - Select version (1 or 2) depending on the version used at the access point.
- **CA Certificates** - Upload a CA certificate to present to the access point for authentication.

Easy Wi-Fi connection with WPS function

WPS (Wi-Fi Protected Setup) refers to the configuration of the encrypted connection between the device and the wireless router. The WPS makes it easy to add new devices to an existing network without entering long passphrases. There are two modes of the WPS connection; the PBC mode and the PIN mode.

Note: If you enable the WPS function, you do not need to configure the parameters or know the key of the wireless connection.

Figure 13: WPS PBC configuration

PBC mode:

PBC (Push-Button-Configuration) allows the user to push a button on both the Access Point and the new wireless client device for configuration.

To enable the PBC function:

1. Select the **Enable WPS** checkbox.
2. Set the connection mode to PBC.

   Note: Each access point must support PBC mode.
3. Check the Wi-Fi router for a WPS button. Push the button, and the indicator near the button starts flashing.

   This means the WPS function is enabled. For detailed operation, see the user guide of the router.
4. Push the WPS button on the camera.

   If there is no WPS button on the camera, click the virtual button on the web interface to enable PBC.
5. Click **Connect**.

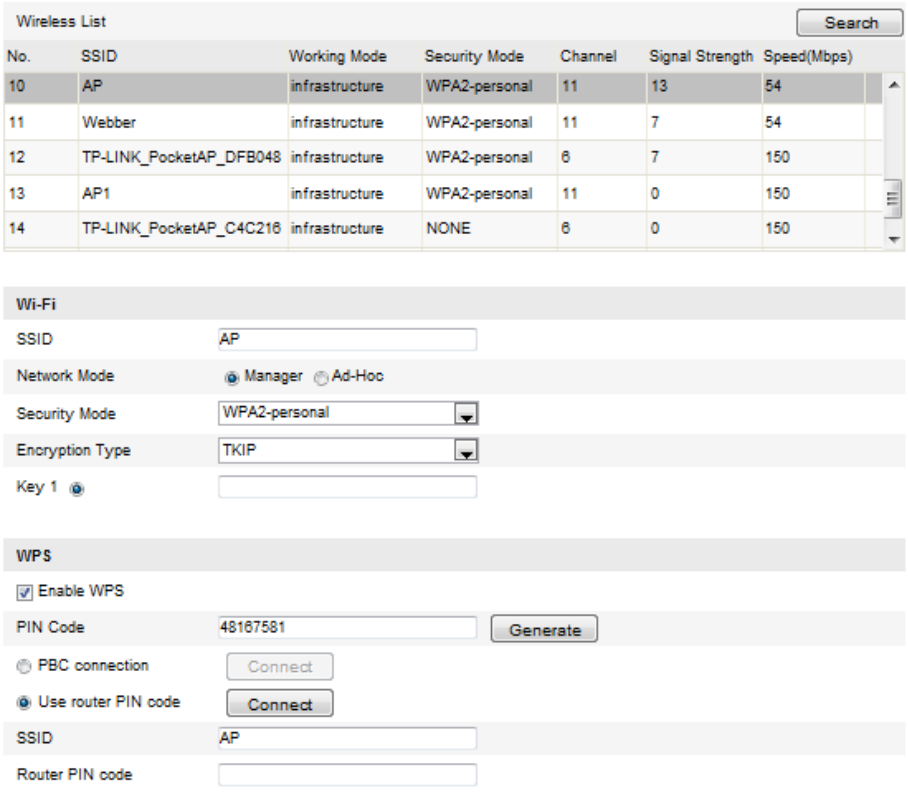
When the PBC mode is enabled in both the router and the camera, the camera and the wireless network connect automatically.

PIN mode:

The PIN (Personal Identification Number) mode requires the pin from either a sticker or the display on the new wireless device. This PIN must then be entered to connect to the network.

To enter PIN mode:

1. Choose a wireless connection on the list and the SSID is shown.


Wireless List
Search
No. SSID Working Mode Security Mode Channel Signal Strength Speed(Mbps)
10 AP infrastructure WPA2-personal 11 13 54
11 Webber infrastructure WPA2-personal 11 7 54
12 TP-LINK_PocketAP_DFB048 infrastructure WPA2-personal 6 7 150
13 AP1 infrastructure WPA2-personal 11 0 150
14 TP-LINK_PocketAP_C4C216 infrastructure NONE 6 0 150
Wi-Fi
SSID AP
Network Mode Manager Ad-Hoc
Security Mode WPA2-personal
Encryption Type TKIP
Key 1
WPS
Enable WPS
PIN Code 48167581 Generate
PBC connection Connect
Use router PIN code Connect
SSID AP
Router PIN code

2. Select Use router Pin code.
3. If the PIN is generated from the router, enter the PIN in the **Router PIN code** field, and then click **Connect**.

   - or -

   You can generate a PIN code using the camera, and then click **Generate**.

   Note: The expiration time for the PIN code is 120 seconds.
4. Enter the router code in the **PIN Code** field.

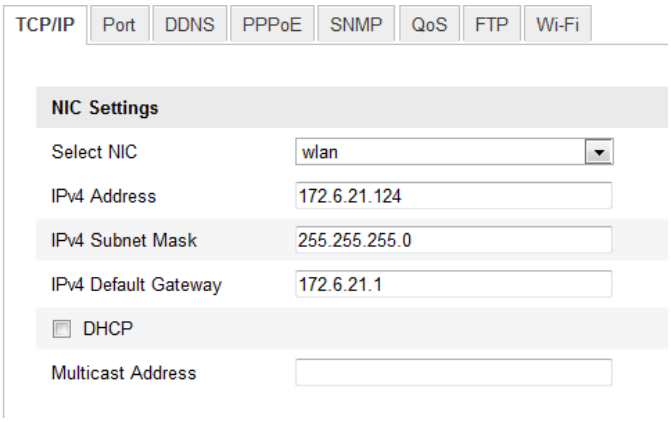
IP property settings for wireless network connection

The default IP address of the wireless network interface controller is 192.168.1.64. When you connect the wireless network you can change the default IP.

To change the default IP:

1. Enter the TCP/IP configuration interface.

   Configuration > Camera Configuration > Network > TCP/IP



2. Set Select NIC as wlan.
3. Customize the IPv4 address, the IPv4 Subnet Mask, the IPv4 Default Gateway, and the Multicast Address.

The setting use the same process as the LAN.

If you do not want to assign the IP address, select the checkbox to enable the DHCP.

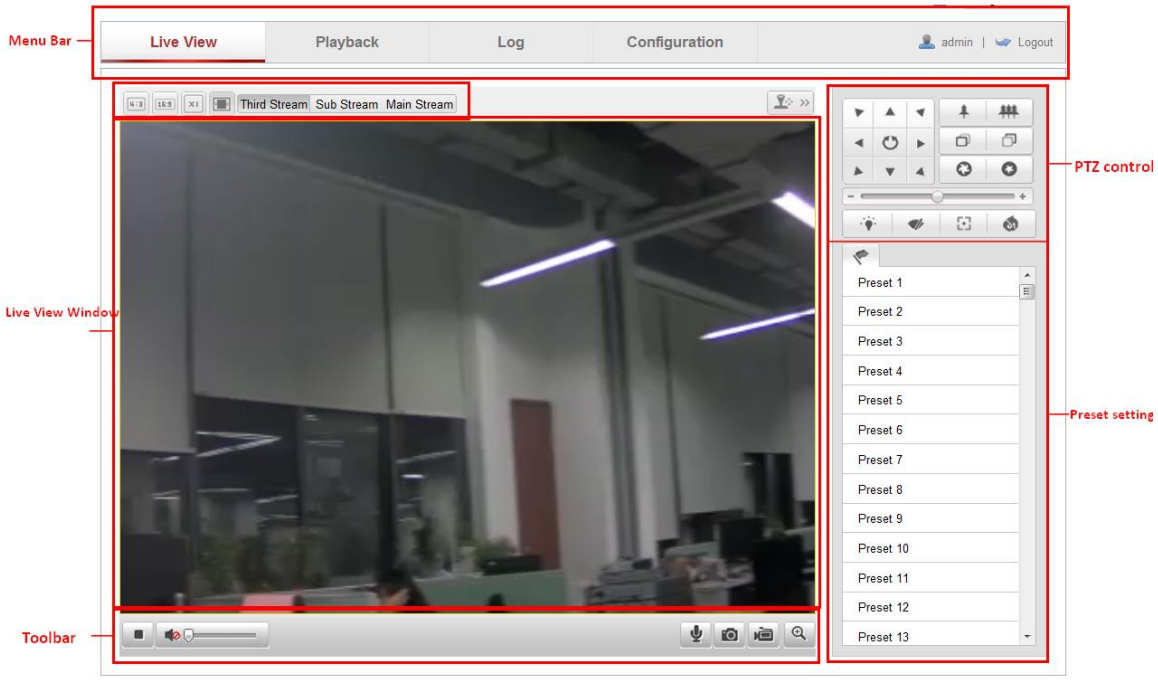
Live View

Live View page

The live video page lets you view live video, capture images, utilize PTZ control, set/call presets, and configure the video parameters.

Log in to the network camera to enter the live view page, or click **Live View** on the menu bar of the main camera page.

Figure 14: Live View page with descriptions



Menu bar: Click each tab to enter the Live View, Playback, Log, and Configuration page.

Live View window: Displays the live video.

Toolbar: Operations of the live view page, e.g., live view, capture, record, audio on/off, two-way audio, etc.

PTZ control: Panning, tilting, and zooming actions of the camera. This also includes the lighter and wiper control (only available if the camera has a PTZ function or an external pan/tilt unit has been installed).

Preset setting/calling: Set and call the presets for the camera (only compatible with PTZ functioning cameras).

Live View parameters: Customizes the image size and stream type of the live video.

Starting live view

Click on the toolbar to start the live view of the camera.

Figure 15: Live View toolbar

Table 1: Description of the Live View toolbar

Icon	Description
	This starts/stops the live view.
	This manually captures the pictures displayed in live view, and then save it them as JPEG files.
	This manually starts/stops recording.
	This turns audio on, adjust volume, and mutes the device.
	This turns on/off the microphone.
	This turns on/off the PTZ.

Note: Before using the two-way audio function or recording with audio, set the **Stream Type** to **Video & Audio** referring to the “Operating PTZ control” on page 53.

Full-screen mode

You can double-click on the live video to switch between full-screen and normal mode.

Recording and capturing pictures manually

In the live view interface, click on the toolbar to capture live images. Click to record live video. The saving paths of the captured pictures and clips can be set on the local configuration tab.

Note: The captured image defaults to saving as a JPEG file in your computer. You can change this in the configuration tab.

Configuring Live View parameters

You can select the stream type and change the image size on the live view page.

To select the stream and adjust the image size:

1. Click the **Main Stream**, **Third Stream**, or **Sub Stream** tab under the menu bar of the live view interface to set the stream type.
2. Click each tab to set the image size to one of the following; 4:3, 16:9, original, or auto fix.

Network camera configuration

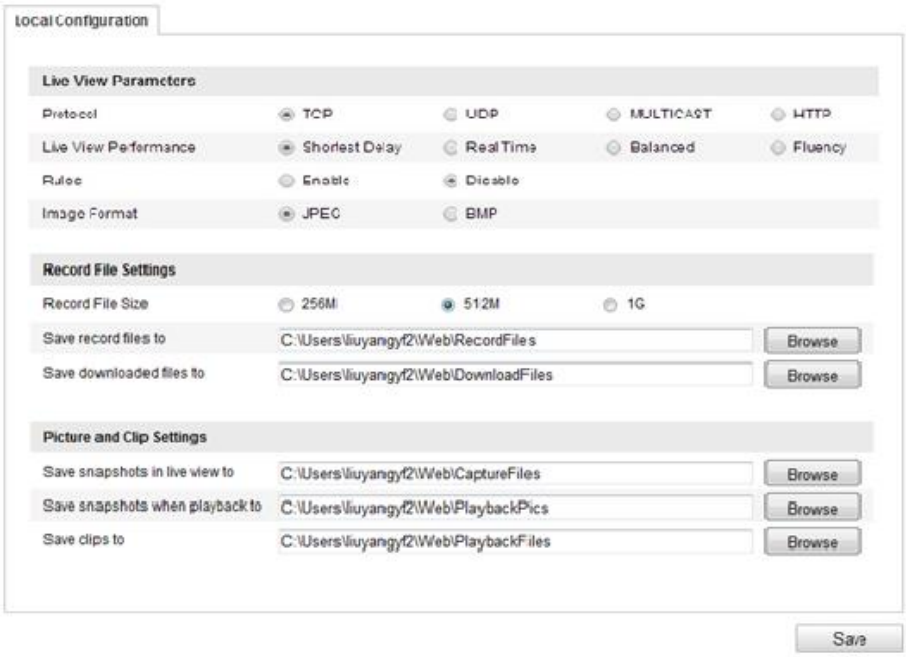
Configuring local parameters

The local configuration refers to the parameters of the live view, record files, and captured pictures.

To configure local parameters:

1. Enter the Local Configuration interface.

   Configuration > **Local Configuration**



2. Configure the following settings:

   Live View parameters: Set the protocol type and live view performance.

   - **Live View performance:** Set the live view performance to Least Delay, Balanced, or Best Fluency
   - **Protocol Type:** Select TCP, UDP, MULTICAST, or HTTP.

     TCP: Ensures the complete delivery of streaming data and better video quality, the real-time transmission will be affected.

     UDP: Provides real-time audio and video streams.

     MULTICAST: It is recommended when using the Multicast function.

     HTTP: Allows the same quality as TCP without setting specific ports for streaming under some network environments.

Record File settings: Set the saving path of the recorded video files. Valid for the record files you recorded with the web browser.

- **Record File Size:** Set the packed size of the manually recorded and downloaded video files to 256 M, 512 M or 1 G.
- **Save record files to:** Set the saving path for the manually recorded video files.
- **Save downloaded files to:** Set the saving path for the downloaded video files in playback mode.

Picture and Clip settings: Set the saving paths of the captured pictures and clipped video files. This is only valid on the pictures captured with the web browser.

- **Save snapshots in live view to:** Set the saving path of the manually captured pictures from live view mode.
- **Save snapshots when playback to:** Set the saving path of the captured pictures from playback mode.
- **Save clips to:** Set the saving path of clipped video files in playback mode.

Note: Click **Browse** to change the directory for saving clips and pictures.

3. Click **Save**.

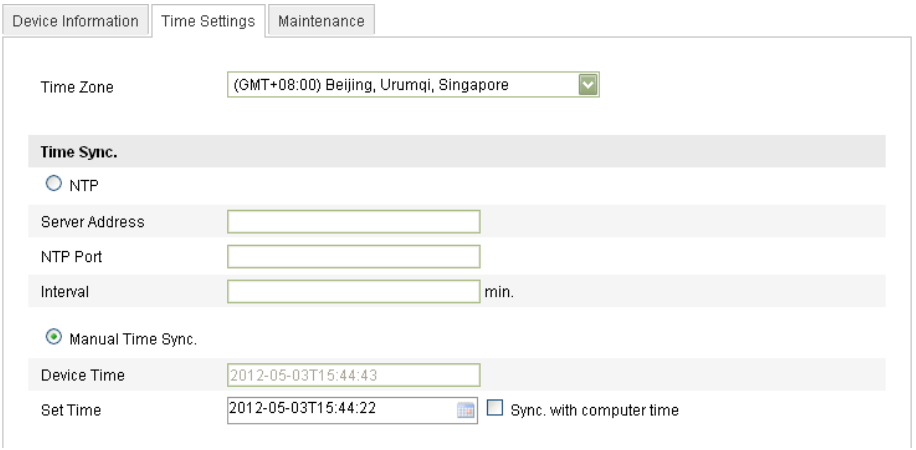
Configuring time settings

Follow the instructions in this section to configure the time synchronization and DST settings.

To configure time settings:

1. Enter the Time Settings interface.

   Configuration > **Camera Configuration** > **System** > **Time Settings**



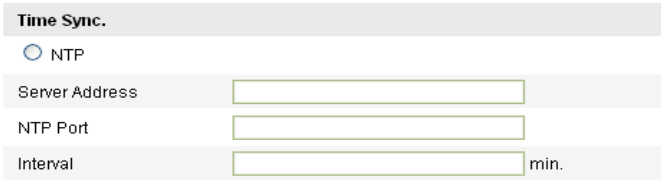
2. Select the Time Zone.

3. Select the checkbox to enable the NTP function.
4. Configure the following settings.

   Server Address: IP address of the NTP server.

   NTP Port: Port of the NTP server.

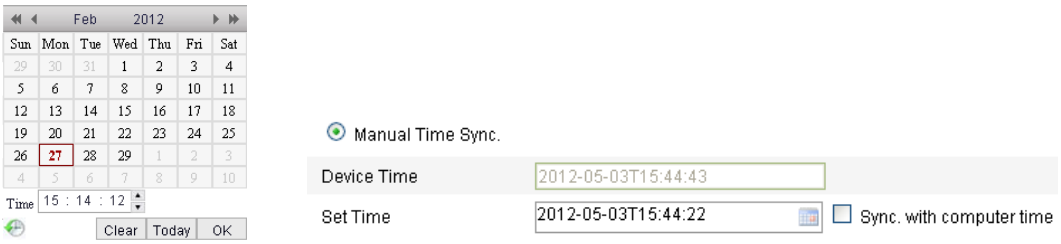
   Interval: The time interval between the two synchronizing actions of the NTP.



   Note: If the camera is connected to a public network, use an NTP server that has a time synchronization function. If the camera is set in a customized network, the NTP software can be used to establish an NTP server for time synchronization.

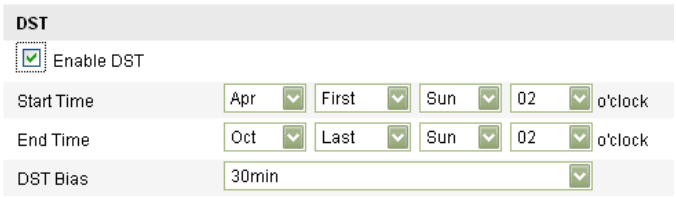
To change Time Synchronization manually:

1. Enable the **Manual Time Sync** function, and then click to set the system time.



   Note: You can select the Sync with computer time checkbox to synchronize the time of the camera with that of your computer.

2. Click **Save**.
3. Click the **DST** tab page to enable the DST function, and then set the date of the DST period.



4. Click **Save**.

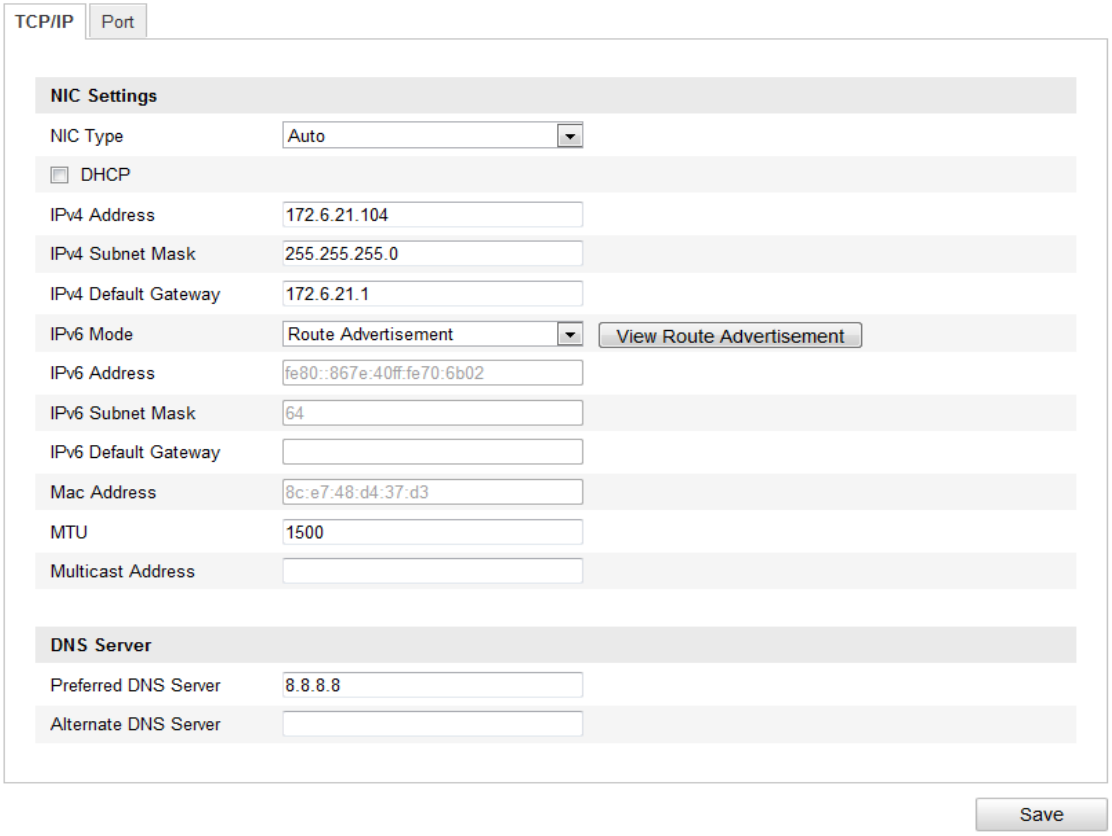
Configuring TCP/IP settings

Configure the TCP/IP settings to operate the camera over the network. The camera supports both the IPv4 and IPv6, both versions may be configured simultaneously without conflicting with each other. At least one IP must be configured.

To configure the TCP/IP settings:

1. Enter the TCP/IP Settings interface.

   Configuration > **Camera Configuration** > **Network** > **TCP/IP**



2. Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings, and Multicast Address.

   Notes

   - The valid value range of MTU is 500 to 1500.
   - The Multicast sends a stream to the multicast group address. It allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, enable the Multicast function of your router.

3. Click **Save**.
4. When prompted, reboot for the settings to take effect.

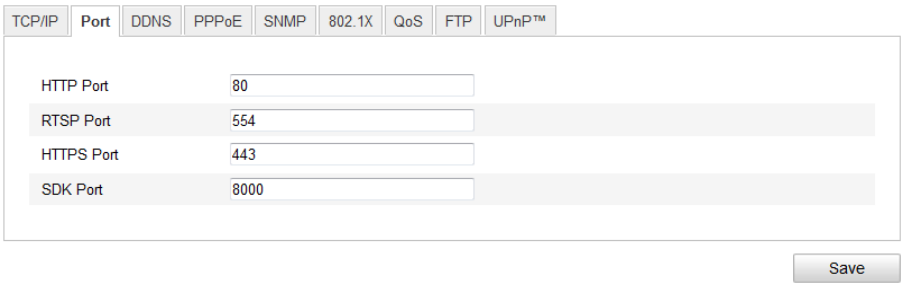
Configuring port settings

You can set the port numbers of the camera, e.g., HTTP port, RTSP port, and HTTPS port.

To configure port settings:

1. Enter the Port Settings interface.

   Configuration > **Camera Configuration** > **Network** > **Port**



2. Set the HTTP port, RTSP port and HTTPS port of the camera.

   HTTP Port: The default port number is 80, it can be changed to a port range from 1024 to 65535.

   RTSP Port: The default port number is 554.

   HTTPS Port: The default port number is 443, it can be changed to a port range from 1024 to 65535.

   SDK Port: The default SDK port number is 8000.

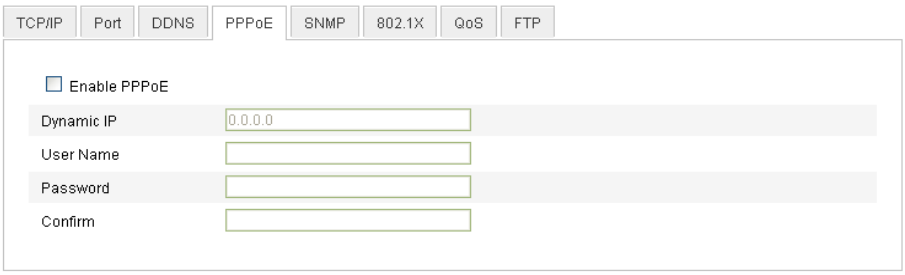
3. Click **Save**.
4. When prompted, reboot for the settings to take effect.

Configuring PPPoE settings

To configure PPPoE settings:

1. Enter the PPPoE Settings interface.

   Configuration > **Camera Configuration** > **Network** > **PPPoE**



2. Select the **Enable PPPoE** checkbox.
3. Enter **User Name**, **Password**, and **Confirm** the password for PPPoE access.

   Note: The User Name and Password is assigned by your ISP.
4. Click **Save**.
5. When prompted, reboot for the settings to take effect.

Configuring DDNS settings

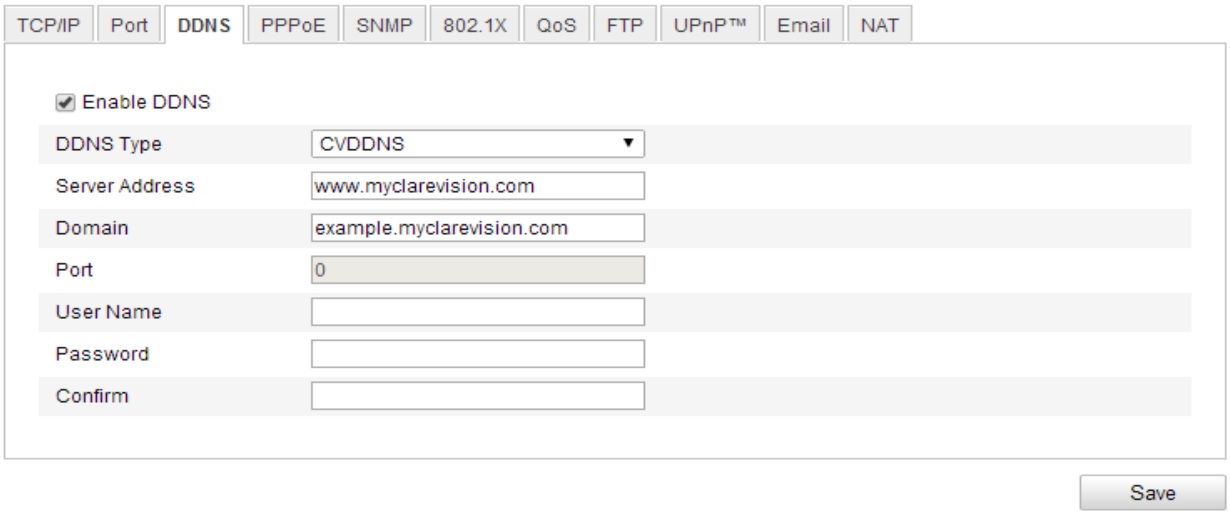
If your camera is set to use PPPoE as its default network connection, use the Dynamic DNS (DDNS) for network access.

Registration on the DDNS server is required before configuring the DDNS settings of the camera.

To configure CVDDNS settings:

1. Enter the CVDDNS Settings interface.

   Configuration > **Camera Configuration** > **Network** > **CVDDNS**



2. Select the **Enable CVDDNS** checkbox.
3. Select **CVDDNS Type**.

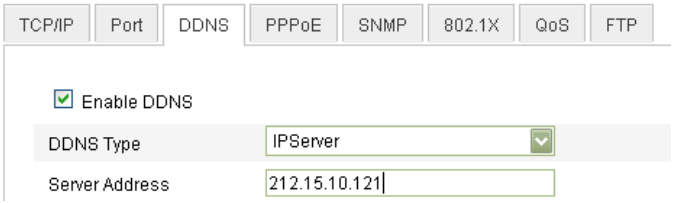
To configure CVDDNS:

1. Enter the **Server Address** of CVDDNS (e.g. myclarevision.com).
2. In the **Domain** text field, enter the domain name obtained from the website.
3. Enter the **Port** of the **CVDDNS** server.
4. Enter the **User Name** and **Password** registered on the CVDDNS website.
5. Click **Save**.

To configure IP server:

1. Enter the Server Address of the IP Server.
2. Click **Save**.

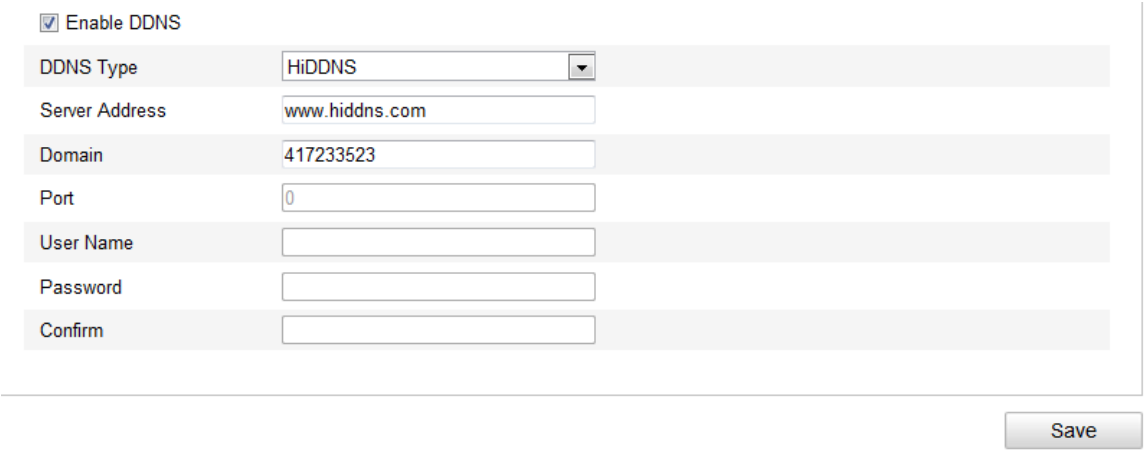
   Note: For the IP Server, you have to apply a static IP, subnet mask, gateway, and the preferred DNS from the ISP. The **Server Address** must match the static IP address of the computer that runs the IP Server software.



   Note: For the US and Canada, you can enter 173.200.91.74 as the server address.

To configure HiDDNS:

1. Select HiDDNS for the the DDNS Type.



2. Enter the Server Address www.hiddns.com.
3. Enter the Domain name of the camera. The domain is the same as the device alias in the HiDDNS server.
4. Click **Save**.
5. When prompted, reboot for the settings to take effect.

Configuring SNMP settings

You can set the SNMP function to get the camera status, parameters, alarm-related information, and manage the camera remotely when it is connected to the network.

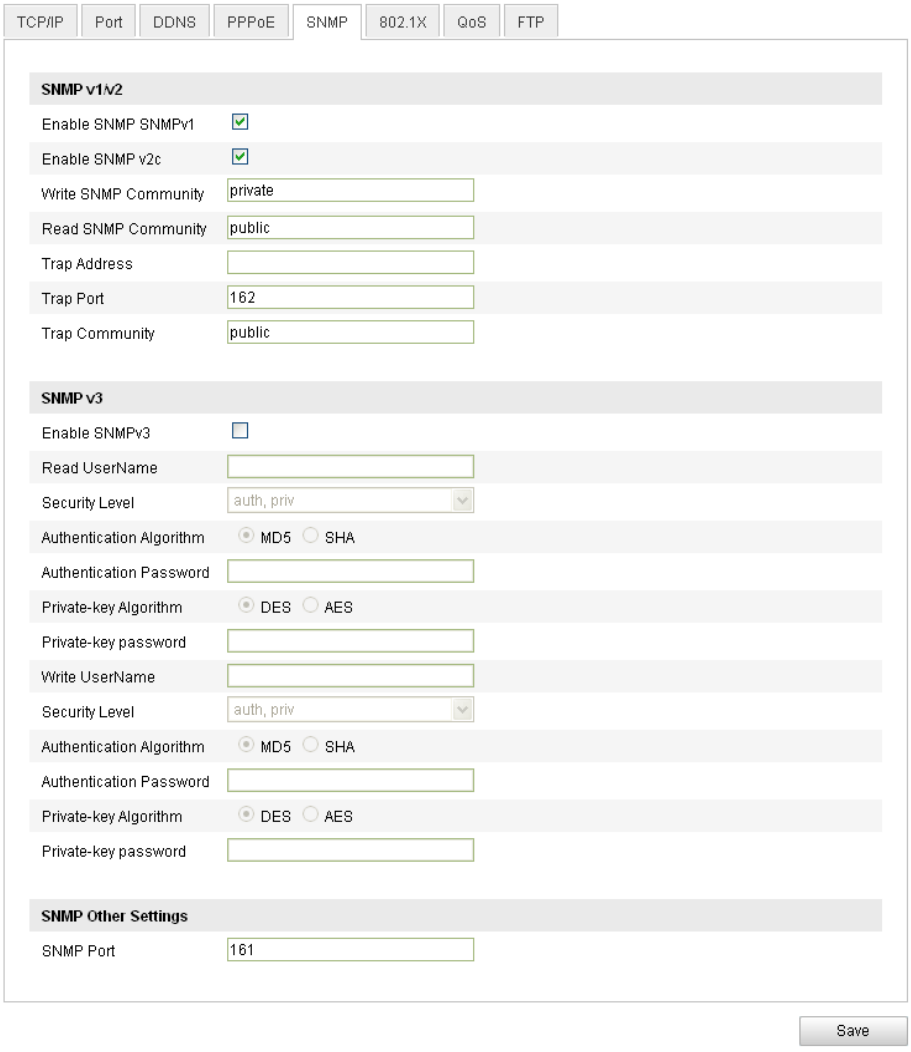
Before setting the SNMP, download the SNMP software and receive the camera information via SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

Note: The SNMP version you select should match the SNMP software. Use the version that corresponds with the security level you required. SNMP v1 provides no security, SNMP v2 requires password for access, and SNMP v3 provides encryption. If you use the third version, HTTPS protocol must be enabled.

To configure SNMP settings:

1. Enter the SNMP Settings interface.

   Configuration > **Camera Configuration** > **Network** > **SNMP**



2. Select the corresponding version checkbox to enable the feature.
3. Configure the SNMP settings.

   Note: The settings of the SNMP software must match the settings configured here.
4. Click **Save**.
5. When prompted, reboot for the settings to take effect.

Configuring 802.1X settings

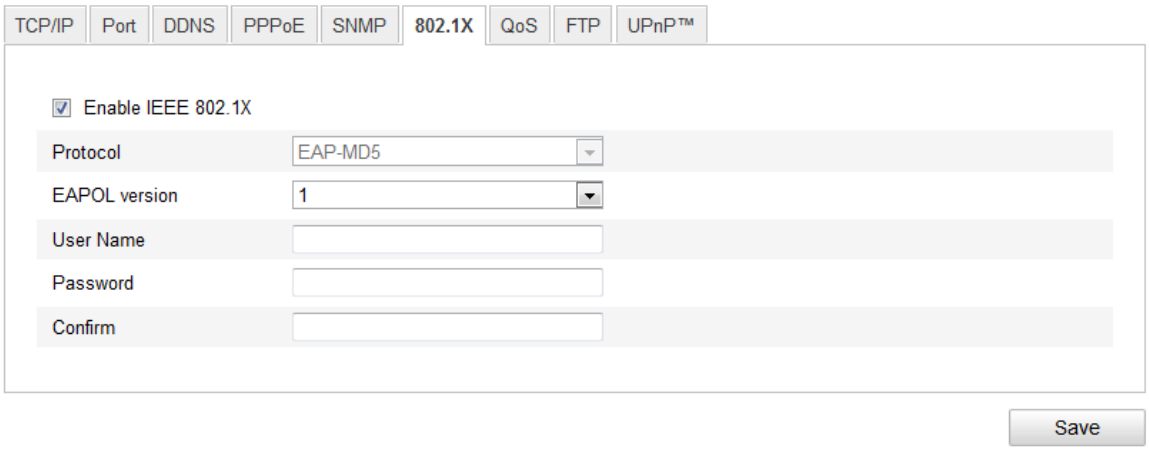
The IEEE 802.1X standard is supported by the network cameras. When the feature is enabled, the camera data is secured. User authentication is needed when connecting the camera to a network protected by the IEEE 802.1X.

The authentication server must be configured. Register and apply a user name and password for 802.1X in the server.

To configure 802.1X settings:

1. Enter the 802.1X Settings interface.

   Configuration > **Camera Configuration** > **Network** > **802.1X**



2. Select the Enable IEEE 802.1X checkbox.
3. Configure the 802.1X settings, including the EAPOL version, user name, and password.

   Note: The EAPOL version must match the router or the switch.
4. Click **Save** to finish the settings.
5. When prompted, reboot for the settings to take effect.

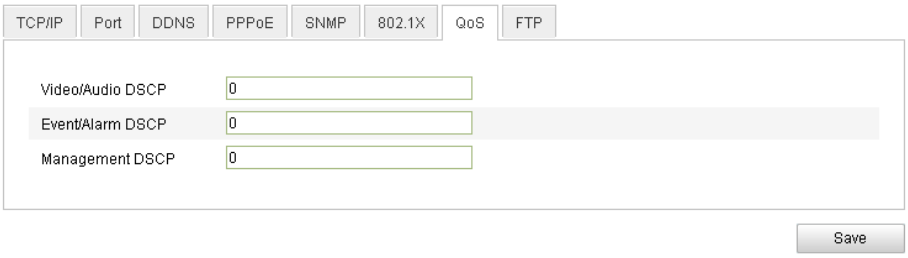
Configuring QoS settings

QoS (Quality of Service) can help solve network delay and congestion by configuring the priority of the data sent.

To configure QoS settings:

1. Enter the QoS Settings interface.

   Configuration > **Camera Configuration** > **Network** > **QoS**



2. Configure the QoS settings, including video/audio DSCP, event/alarm DSCP, and Management DSCP.

   Notes

   - DSCP refers to the Differentiated Service Code Point; and the DSCP value is used in the IP header to indicate the priority of the data.
   - The valid value range of the DSCP is 0 to 63. The larger the DSCP value, the higher the priority is.

3. Click **Save**.
4. When prompted, reboot for the settings to take effect.

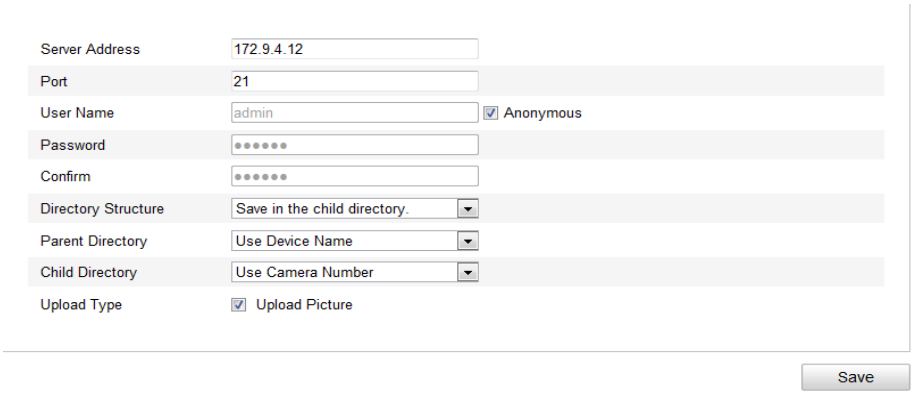
Configuring FTP settings

You can configure the FTP server related information to enable the uploading of the captured images to the FTP server. The captured pictures can be triggered by events or a timing snapshot task.

To configure FTP settings:

1. Enter the FTP Settings interface.

   Configuration > **Camera Configuration** > **Network** > **FTP**



2. Enter the user name and password required to log into the FTP server in the corresponding fields.
3. In the Directory Structure field, select the root directory, parent directory, or child directory.

   When the parent directory is selected, you have the option to use the Device Name, Device Number, or Device IP for the name of the directory.

   When the Child Directory is selected, you can use the Camera Name or Camera No. as the name of the directory.
4. Select the Upload Type checkbox to enable uploading the captured image to the FTP server.
5. Select the Anonymous checkbox to enable anonymous access to the FTP server.

   When you select this checkbox, the user name and password will not be requested.

   Note: The anonymous access function must be supported by the FTP server.
6. Click **Save**.

Note: If you want to upload the captured images to the FTP server, you must enable the continuous snapshot or the event-triggered snapshot on the Snapshot page.

Configuring UPnP settings

Universal Plug and Play (UPnP) is a networking architecture that provides compatibility among networking equipment, software, and other hardware devices. The UPnP protocol allows devices to connect seamlessly and simplifies the implementation of networks in the home and corporate environments.

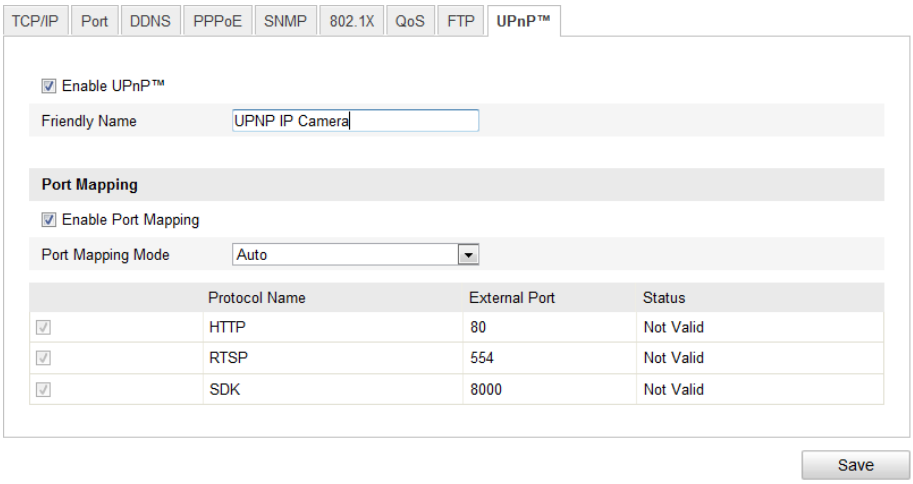
With the function enabled, the camera is connected to the Wide Area Network via the router, you do not need to configure port mapping for each port.

To configure UPnP settings:

1. Enter the UPnP settings interface.

   Configuration > **Camera Configuration** > **Network** > **UPnP**

2. Select the Enable UPnP checkbox. This enables the Friendly Name field.
3. In the Friendly Name field, enter the name of the device.

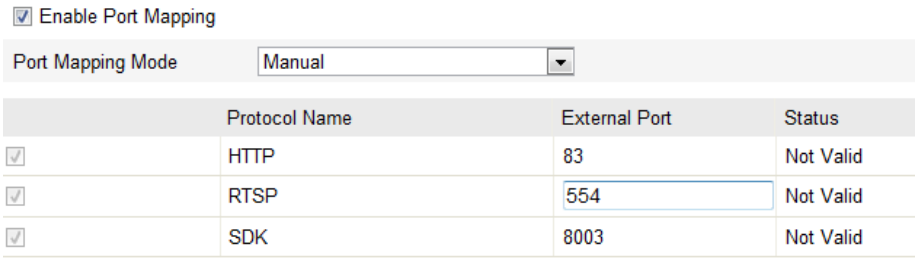


4. From the Port Mapping Mode drop-down, choose one of the following:

   Auto for port mapping with the default port numbers.

   - or -

   Manual for port mapping with the customized port numbers.



5. Click **Save**.

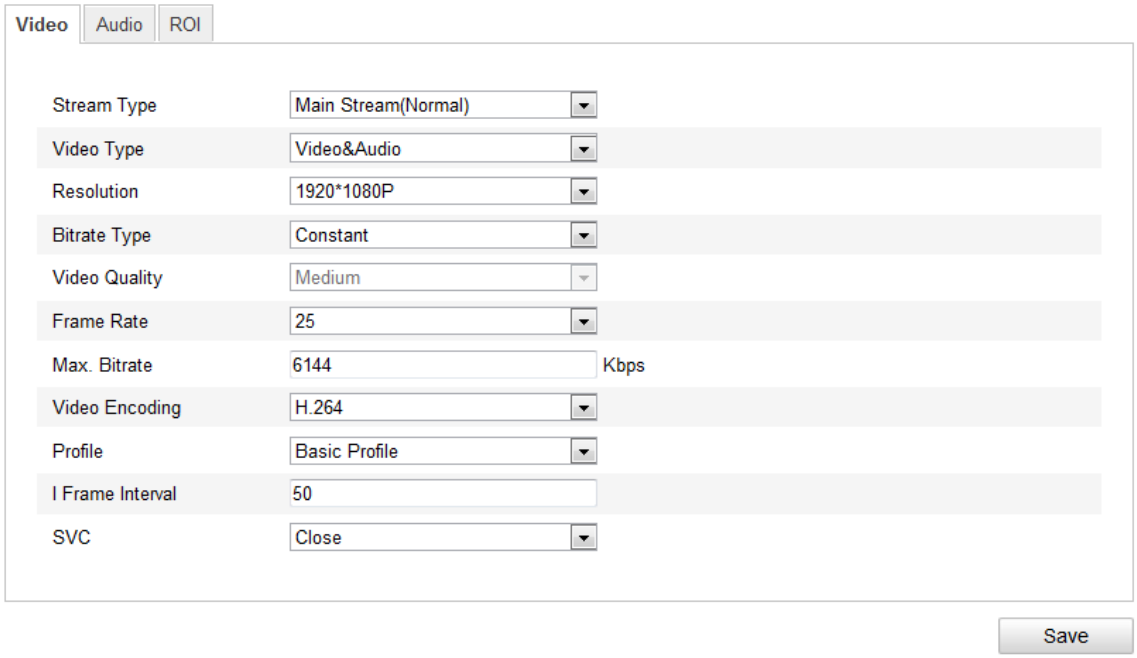
Configuring video settings

Customizing the video settings allows for better quality images based on the custom needs of that video stream.

To configure video settings:

1. Enter the Video settings interface.

   Configuration > **Camera Configuration** > **Video/Audio** > **Video**



2. In the **Stream Type** field, select **Main Stream** (normal), **Sub-Stream,** or **Third Stream**.

   Note: Main Stream is optimal for recording and live viewing with good bandwidth. Sub Stream and Third Stream can be used for live viewing with limited bandwidth.

3. You can customize the following parameters for the selected Stream.

   Video type: Set the stream type to video stream, or video and audio composite stream. The audio signal will be recorded only when the Video Type is Video and Audio.

   Resolution: Select the resolution of the video output.

   Bitrate type: Set the bitrate type to constant or variable.

   Video quality: When the bitrate type is set to Variable, six levels of video quality are available.

   Frame rate: Set the frame rate to 1/16 to 25 fps. The frame rate describes the frequency at which the video stream is updated. It is measured by frames per second (fps). A higher frame rate is beneficial when there is movement in the video stream, it maintains the image quality throughout.

   Maximum bitrate: Set the maximum bitrate from 32 to 16384 Kbps. The higher the value, the higher video quality. Bandwidth requirements go up with the video quality.

   Video encoding: When the Stream Type of the camera is set to main stream, the Video encoding standard can be set to H.264.

   When the Stream type of the camera is sub-stream, the Video Encoding standard can be set to H.264, MJPEG.

Profile: Basic profile, Main Profile, and High Profile are selectable for coding.

I Frame interval: Set the I-Frame interval from 1 to 400.

SVC: Scalable video coding (SVC) is an extension of the H.264 /AVC standard. The technology encodes the video signal with layers, a basic layer and several enhanced layers. It adapts to the network condition to transfer different video streams. For example, when the bandwidth is limited, only the basic layer of data is encoded and transferred. Enable this function when you want to view the video with several terminals, for example - a smartphone, or a computer with an IP network.

4. Click **Save**.

Configuring audio settings

Customizing the audio settings allows for better quality sounds based on the custom needs of that audio stream.

To configure audio settings:

1. Enter the Audio Settings interface.

   Configuration > **Camera Configuration** > **Video/Audio** > **Audio**

2. From the Audio Encoding drop-down list, select one of the following:

   G.711 ulaw
   G.711 alaw
   G.726
   MP2L2

3. From the Audio Input drop-down list, select one of the following:

   MicIn (microphone)
   Linein (pickup)

4. Click **Save**.

Configuring ROI encoding

ROI (region of interest) encoding lets you discriminate the ROI and background information in comparison. This means that the technology assigns more encoding resources to the region of interest to increase the quality of the ROI view.

Note: Not all cameras support this function.

To configure ROI encoding:

1. Enter the ROI settings interface.

   Configuration > **Camera Configuration** > **Video/Audio** > **ROI**
2. Draw the region of interest on the image. Up to four regions can be drawn.
3. Select the stream type to set ROI encoding.
4. Select the ROI type.

   Fixed region: Fixed region ROI is encoding for a manually configured area. You can choose the Image Quality Enhancing level for ROI encoding, and name the ROI area.

   Dynamic tracking: Dynamic tracking ROI is defined by intelligent analysis, such as human face detection. You can choose the Image Quality Enhancing level for the ROI encoding.
5. Click **Save**.

Configuring image parameters

Image parameters cover display, OSD, text over-lay, privacy mask, and picture over-lay settings.

Configuring display settings

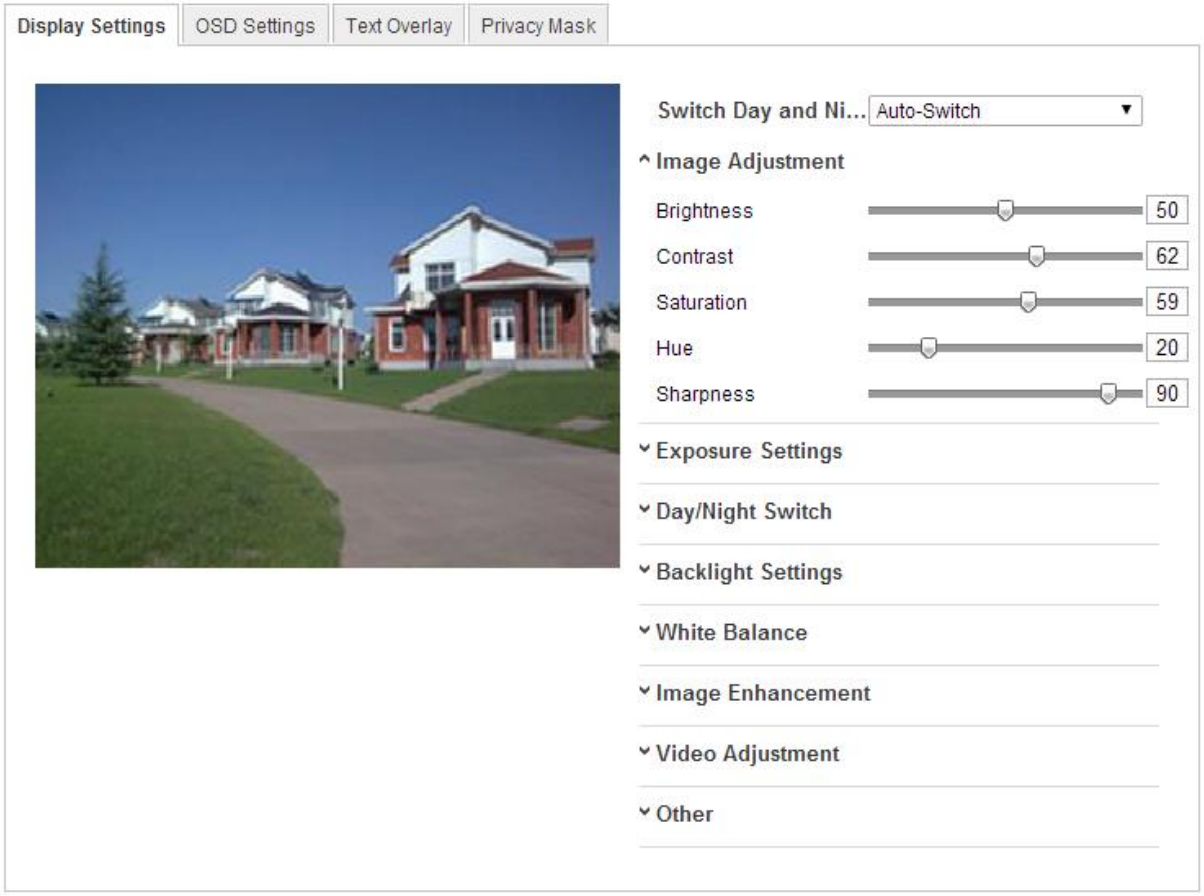
You can set the image quality of the camera, including brightness, contrast, saturation, hue, sharpness, etc.

Note: The Display parameters vary depending on the camera model.

To configure display settings:

1. Enter the Display Settings interface.

   Configuration > **Camera Configuration** > **Image** > **Display Settings**
2. Set the image parameters of the camera.



Overexposure prevention: Enable or disable the function in this field.

Exposure time: Value ranges from 1/3 to 1/100,000 s. Adjust it according to the light condition.

Iris mode: Select from Auto and Manual.

Auto iris Level: If you choose the auto iris mode, you can set the auto iris level.

Video standard: Select from 50 Hz and 60 Hz. Choose according to the different video standards; normally 50 Hz for the PAL standard and 60 Hz for the NTSC standard.

Day/Night switch: Choose Day, Night, Auto, Schedule, or Triggered by Alarm input.

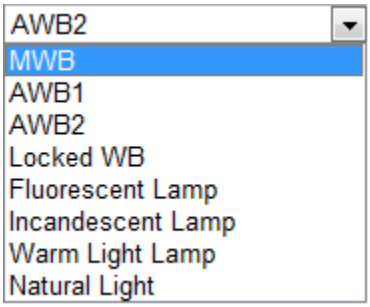
Sensitivity: If you choose the auto day/night switch, you can set the sensitivity of the switch as high, normal, and low.

Mirror: The mirror function enables you to view another aspect of the image. You can flip the image horizontally and vertically.

WDR: Wide dynamic range can be used when there is a high contrast of bright area and dark area in a scene.

BLC area: BLC area is the sense of the light intensity, select Close, Up, Down, Left, Right, and Center.

White balance: The below figure shows the white balance options. Select according to the real condition. For example, if there is a fluorescent lamp in the surveillance scene, select the white balance type as Fluorescent Lamp.



Digital noise reduction: Select Close, Normal, or Expert Mode.

Noise reduction level: Adjusts the noise reduction level. This is only valid when the DNR function is enabled.

Scene mode: Select indoor or outdoor.

HLC: The high light compression function can be used when there are strong lights in the scene that affect the image quality.

Grey Scale: You can choose the range of the grey scale as [0 to 255] or [16 to 235].

Corridor mode: To use of the 16:9 aspect ratio, enable the corridor mode when you use the camera in a narrow view scene.

Note: When installing, turn the camera to the 90 degrees or rotate the 3-axis lens to 90 degrees, and then set the corridor mode as on. You will get a normal view of the scene with 9:16 aspect ratio.

Configuring OSD Settings

You can customize the camera name and time displayed on the screen.

To configure OSD settings:

1. Enter the OSD Settings interface.

   Configuration > **Camera Configuration** > **Image** > **OSD Settings**

2. Select the corresponding checkbox to select the display of camera name, date, or week if required.
3. In the Camera Name field, enter the name of the camera.
4. Set the Time Format, Date Format, Display Mode, and OSD Size from the drop-down lists.
5. In the live view window, use the mouse to click and drag the text frame (e.g., IP Camera 01) to adjust the OSD position.
6. Click **Save**.

Configuring text overlay settings

You can customize the text overlay.

To configure text overlay settings:

1. Enter the Text Overlay Settings interface.

   Configuration > **Camera Configuration** > **Image** > **Text Overlay**

2. Select the box in front of the first textbox to enable the on-screen display.
3. Input the characters in the textbox.
4. Use the mouse to click and drag the red text frame in the live view window to adjust the text overlay position.
5. Click **Save**.

   Note: You can configure up to four text overlays.

Configuring privacy mask

Privacy masks let you cover certain areas on the live video to prevent zones in the surveillance area from being viewed or recorded.

To configure privacy mask

1. Enter the Privacy Mask Settings interface.

   Configuration > **Camera Configuration** > **Image** > **Privacy Mask**

2. Select the box of **Enable Privacy Mask** check box.
3. Click **Draw Area**.
4. Click and drag the mouse in the live video window to draw the mask area.

   Note: You are allowed 4 areas on the same image.
5. Click **Stop Drawing** to finish drawing.
   – or –
   Click **Clear All** to clear all of the areas you set without saving them.
6. Click **Save**.

Configuring picture overlay

Picture overlay lets you overlay a picture on the image.

To configure picture overlay:

1. Enter the Picture Overlay Settings interface.

   Configuration > **Camera Configuration** > **Image** > **Picture Overlay**

2. Click **Browse** to add a picture from your PC.
3. Click **Upload**.
4. Slect the **Enable Picture Overlay** checkbox.
5. Set the **X** and **Y Coordinate** values for the location of the picture on the image.
6. Set the **Picture Width** and **Height** to adjust the size of the picture.

Configuring and handling alarms

This section explains the configuration of the network camera to respond to alarm events, including motion detection, external alarm input, video loss, video tampering, and exception. These events can trigger the alarm actions to Notify Surveillance Center, Send Email, etc. For example, when an external alarm is triggered, the network camera sends a notification to an email address.

Configuring motion detection

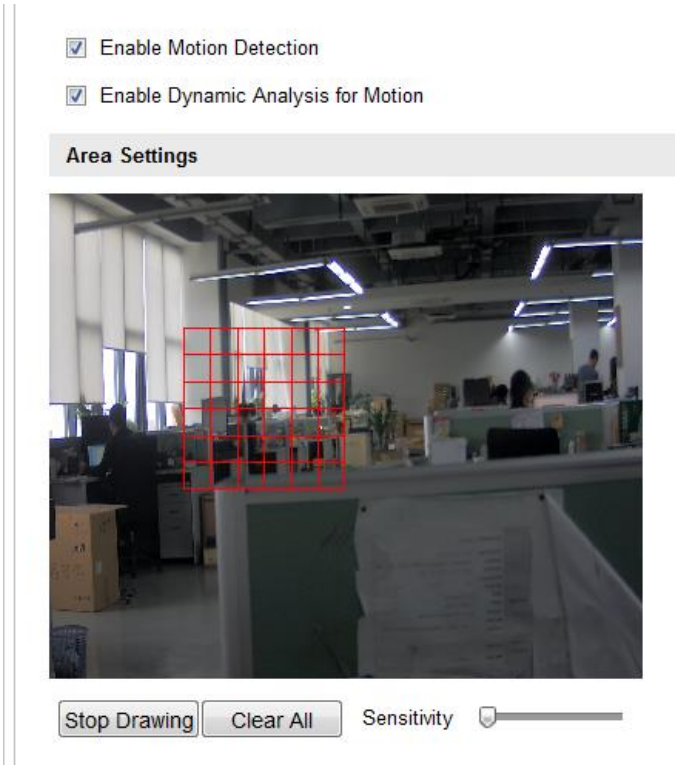
Motion detection is a feature that can take alarm response actions and record the video for the motion occurred in the surveillance scene.

To set the motion detection area:

1. Enter the motion detection settings interface.

   Configuration > **Camera Configuration** > **Events** > **Motion Detection**

2. Select the Enable Motion Detection checkbox.



3. Click **Draw Area**, and then click and drag the mouse on the live video image to draw a motion detection area.
4. Click **Stop Drawing** to finish drawing.

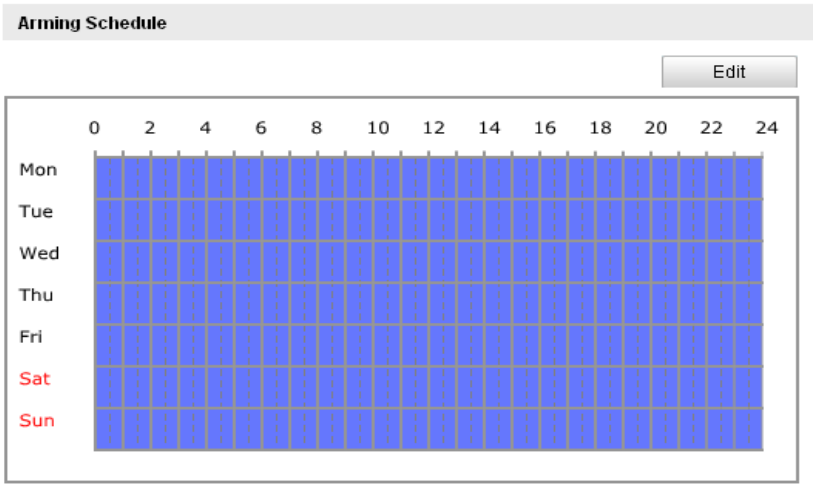
   – or –

   Click **Clear All** to clear all of the areas without saving.
5. (Optional) Move the Sensitivity slider to set the sensitivity of the detection.

Arming schedule for motion detection

You can set the arming schedule for motion detection.

Figure 16: Arming schedule screen

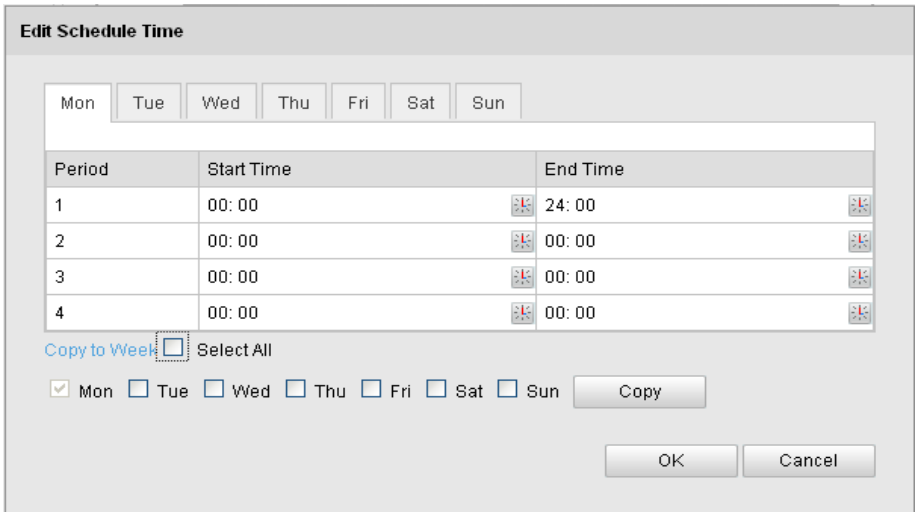


To set the arming schedule for motion detection:

1. Click **Edit**.
2. Select the day.
3. Set the time.
4. After you set the arming schedule, you can copy the schedule to other days.
5. Click **OK** to save the settings.

Note: The time of each period cannot be overlapped. Four periods can be configured each day.

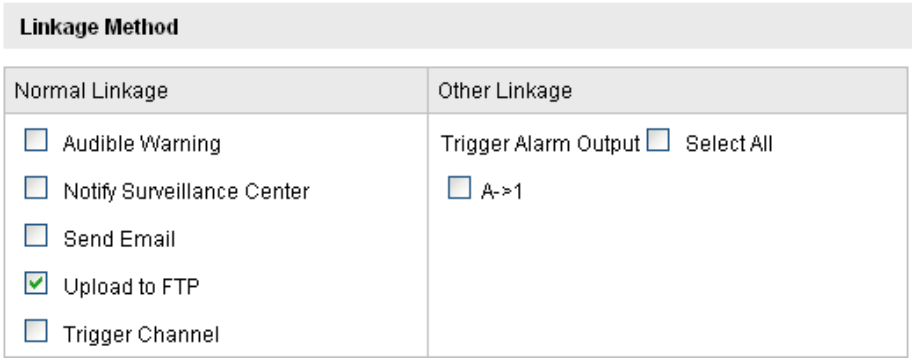
Figure 17: Edit table for the arming schedule



Set the alarm actions for motion detection.

You can specify the linkage method when an event occurs.

Figure 18: Linkage method selection



To set the alarm actions:

1. Select the desired linkage method checkbox. Linkage methods include Audible warning, notify surveillance center, send email, upload to FTP, and trigger channel.

   Audible warning: This triggers the audible warning locally.

   Notify surveillance center: This sends an exception or alarm signal to remote management software when an event occurs.

   Send email: This sends an email with the alarm information to users when an event occurs.

   Upload to FTP: This captures an image when the alarm is triggered and uploads the picture to a FTP server.

   Trigger channel: The video will be recorded when motion is detected. Set the recording schedule to realize this function.

   Trigger alarm output: This triggers one or more external alarm outputs when an event occurs.

Configuring video tampering alarm

You can configure the camera to trigger the alarm and take the alarm response action when the lens is covered.

To configure the video tampering alarm:

1. Enter the Video Tampering settings interface.

   Configuration > **Camera Configuration** > **Events** > **Video Tampering**

2. Select the **Enable Video Tampering** checkbox to enable the tamper-proof detection.
3. Set the tamper-proof area.
4. Click **Edit**.
5. Set the linkage method for video tampering. Select the checkbox for Audible warning, notify surveillance center, or send email.
6. Click **Save**.

Handling exception

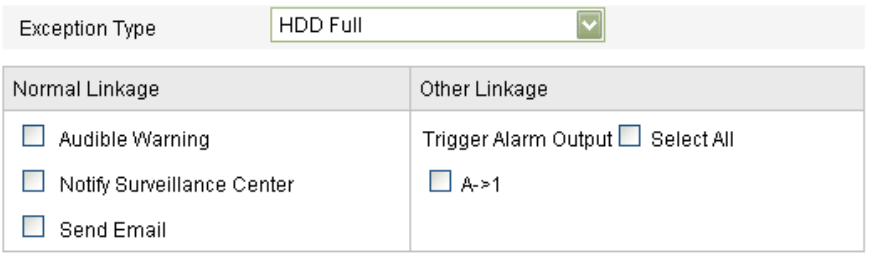
The exception type can be HDD full, HDD error, network disconnected, IP address conflicted, or illegal login to the cameras.

To configure handling exceptions:

1. Enter the Exception Settings interface.

   Configuration > **Camera Configuration** > **Events** > **Exception**

   Select the checkbox to set the actions taken for the Exception alarm.



2. Click **Save**.

Email sending triggered by alarm

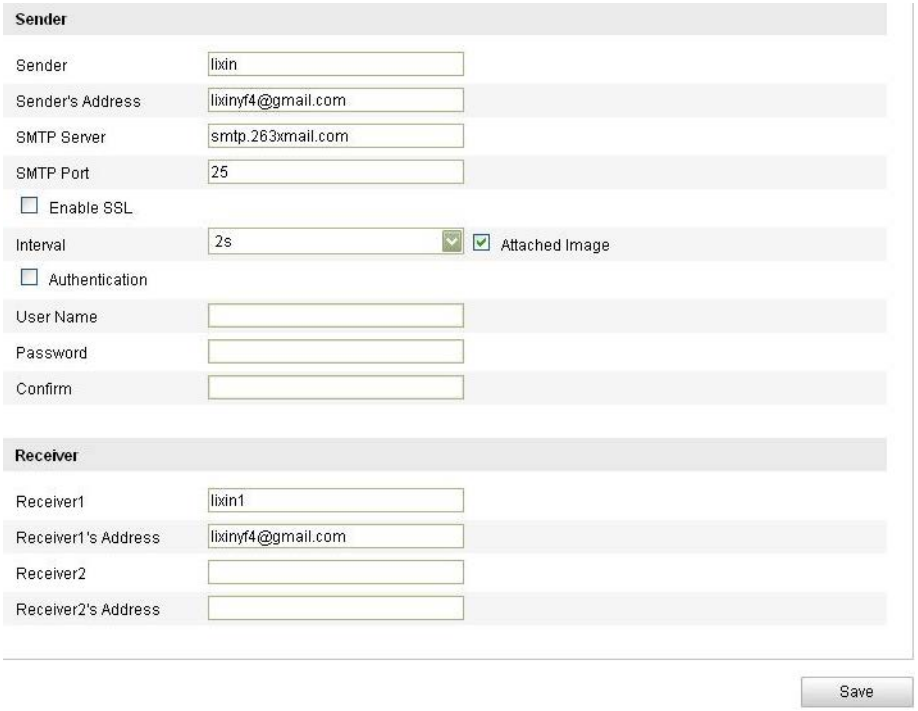
The system can be configured to send an Email notification to all designated receivers if an alarm event is detected – for example, motion detection event, video loss, video tampering, etc.

Note: Before using the Email function, configure the DNS server settings. Go to Configuration > Network > TCP/IP.

To send email triggered by an alarm:

1. In TCP/IP, set the IPv4 /IPv6 Address, IPv4 /IPv6 Subnet Mask, IPv4 /IPv6 Default Gateway, and the Preferred DDNS Server.
2. Enter the Email Settings interface.

   Configuration > **Camera Configuration** > **Network** > **Email**



3. Configure the following settings.

   Sender: The name of the email sender.

   Sender's address: The email address of the sender.

   SMTP server: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

   SMTP port: The default TCP/IP port for SMTP is 25 (not secured). And the SSL SMTP port is 465.

   Enable SSL: Select the checkbox to enable SSL, if the SMTP server requires it.

Attached image: Select the checkbox Attached Image to send the emails with attached alarm images.

Interval: The interval refers to the time between the actions of sending attached pictures.

Authentication (optional): If your email server requires authentication, select this checkbox to use authentication to log in to this server and enter the login user name and password.

Receiver: The name of the user to be notified.

Receiver's address: The email address of user to be notified.

4. Click **Save**.

Configuring snapshot settings

You can configure scheduled snapshots and event-triggered snapshots. The captured images can be stored in the SD card, the netHDD, or uploaded into an FTP server.

To configure basic snapshot settings:

1. Enter the Snapshot Settings interface

   Configuration > **Camera Configuration** > **Storage** > **Snapshot**
2. Select the **Enable Timing Snapshot** checkbox to enable continuous snapshots.
3. Select the **Enable Event-triggered Snapshot** checkbox to enable event-triggered snapshots.
4. Select the quality of the snapshots.
5. Set the time interval between snapshots.
6. Click **Save**.

Uploading to FTP

Follow the instructions below to upload the snapshots to FTP.

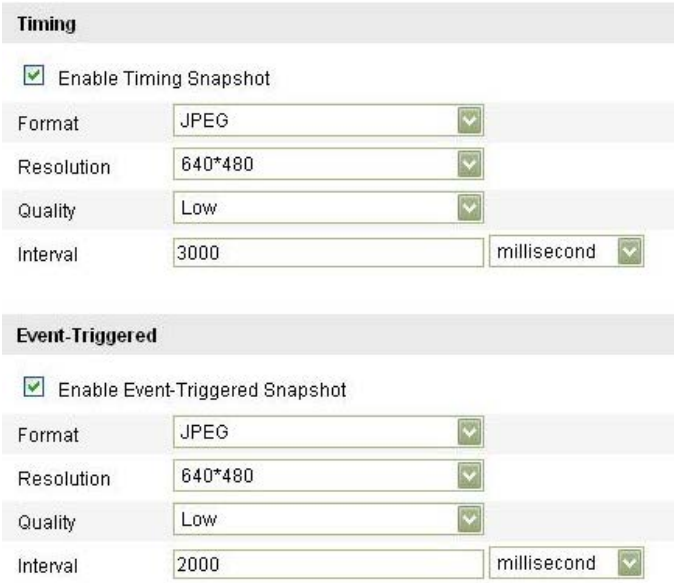
To upload continuous snapshots to FTP:

1. Enter the FTP settings interface

   Configuration > **Camera Configuration** > **Storage** > **FTP**
2. Configure the FTP settings, and then select the Upload Picture checkbox in the FTP Settings interface.
3. Select the **Enable Timing Snapshot** checkbox.

To upload event-triggered snapshots to FTP:

1. Configure the FTP settings and select the Upload Picture checkbox in the FTP Settings interface.
2. Select the Upload to FTP checkbox in the Motion Detection Settings.
3. Select the **Enable Event-triggered Snapshot** checkbox.



Configuring other alarms

This section is for cameras that support external wireless alarms (access control alarm), and manual alarm by remote control.

The wireless alarm is the function of the camera to communicate to a wireless alarm devices such as the access control. The remote control or other remote alarm devices must be compatible and learn each other's remote signal to communicate.

Manual Alarm/Emergency Alarm

Some cameras support the manual alarm by remote control. These can be manually triggered and linked to the audio warning. Press and hold the manual alarm button on the remote control for 2 seconds to trigger the audio warning.

Notes

- The manual alarm is enabled and armed by default and is not user-configurable.
- The manual alarm triggered record will be started if the manual alarm is triggered on the defined recording schedule, and will be stopped in 10 seconds after the manual alarm stops.

Arming or disarming the camera

This section if for supported cameras only. Follow the steps below to configure all-day arming for the camera with the wireless alarm, PIR alarm, motion detection, video tampering, etc.

Notes

- The emergency alarm is enabled and armed by default.
- The arming and disarming function can be set by the remote control.

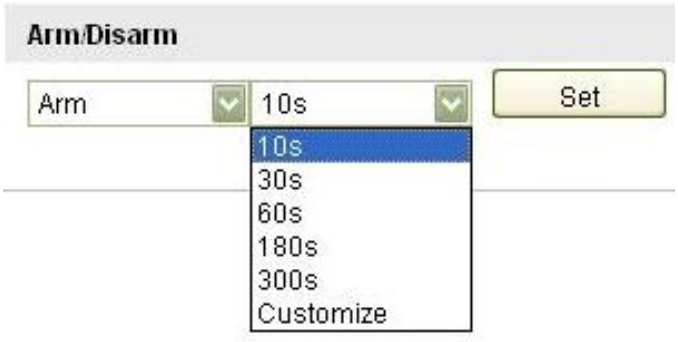
To arm the camera:

1. Enter the Remote Control interface.

   Configuration > **Camera Configuration** > **System** > **Remote Control**

2. Select **Arm** from the **Arm/Disarm** drop-down list.
3. Set the arming delay.

   Note: Arming delay refers to a time delay to arm the camera after you set it. You can set the delay as 10 seconds, 30 seconds, 1 minute, 3 minutes, 5 minutes, or customize the delay time.



4. Click **Set** to arm the camera.

To disarm the camera:

In the Remote Control interface, select **Disarm** from the **Arm/Disarm** drop-down list and click **Set** to disarm the camera.

Note:

- You can press the Arm/Disarm button on the remote control to arm/disarm the camera if the camera has already studied the remote control.
- The arming indicator glows red when the camera is armed and glows blue when it is disarmed.

Configuring PTZ

This section explains the PTZ functions of the network camera. This enables the pan/tilt/zoom control of the camera.

To realize PTZ control, the camera connected to the network must support the PTZ function, or a pan/tilt unit must be installed on the camera. Properly set the PTZ parameters in the **Camera Configuration** settings page.

Operating PTZ control

In the live view interface, use the PTZ control buttons to realize pan/tilt/zoom control of the camera.

To realize PTZ control, the camera connected to the network must support the PTZ function or a pan/tilt unit must be installed on the camera. Properly set the PTZ parameters on RS-485 settings page.

PTZ control panel

To control PTZ:

1. On the live view page, click « to show the PTZ control panel and » to hide it.
2. Click the direction buttons to control the pan/tilt movements.

3. Click the zoom/iris/focus buttons to realize lens control.

   Note: There are 8 direction arrows (△, ▽, ◁, ▷, ▷, ◁, ▷, ◁) in the live view window.

Table 2: Description of the PTZ control panel

Icon	Description
	Zoom in/out
	Focus near/far
	Iris open/close
	Light on/off

	Wiper on/off
	One-touch focus
	Initialize lens
	Pan/tilt speed

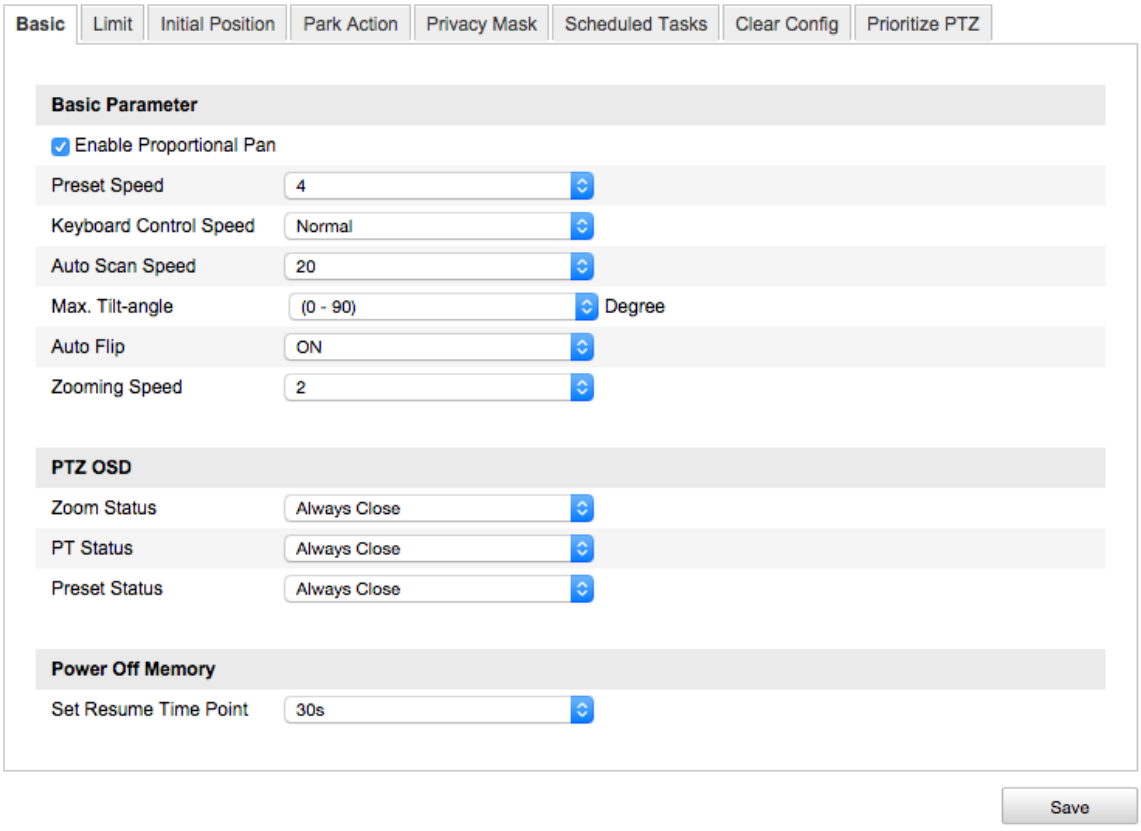
Configuring the basic PTZ settings

The Basic settings lets you change basic parameters, speeds, and OSD.

To configure the basic settings interface:

1. Enter the Basic settings interface.

   Configuration > **Camera Configuration** > **PTZ** > **Basic**



2. Select the Enable Proportional Pan checkbox. This will enable customization of the following parameters.

   Preset Speed: Select an option 1 to 8.

   Keyboard Control Speed: Select an option; Low, Normal, or High.

   Auto Scene Speed: Select an option 1 through 40.

Max. Tilt-angle: Select either -5 to 90, -4 to 90, -3 to 90, -2 to 90, -1 to 90, and 0 to 90.

Auto Flip: Select either On or Off.

Zooming Speed: Select 1, 2, or 3.

3. In the PTZ OSD fields, customize the following.

   Zoom Status: Select Always Open, Always Closed, 2 seconds, 5 seconds, and 10 seconds.

   PT Status: Select Always Open, Always Closed, 2 seconds, 5 seconds, and 10 seconds.

   Preset Status: Select Always Open, Always Closed, 2 seconds, 5 seconds, and 10 seconds.

4. In the **Power Off Memory** field select one of the following, Disable, 30 seconds, 60 seconds, 300 seconds, 600 seconds.
5. Click **Save**.

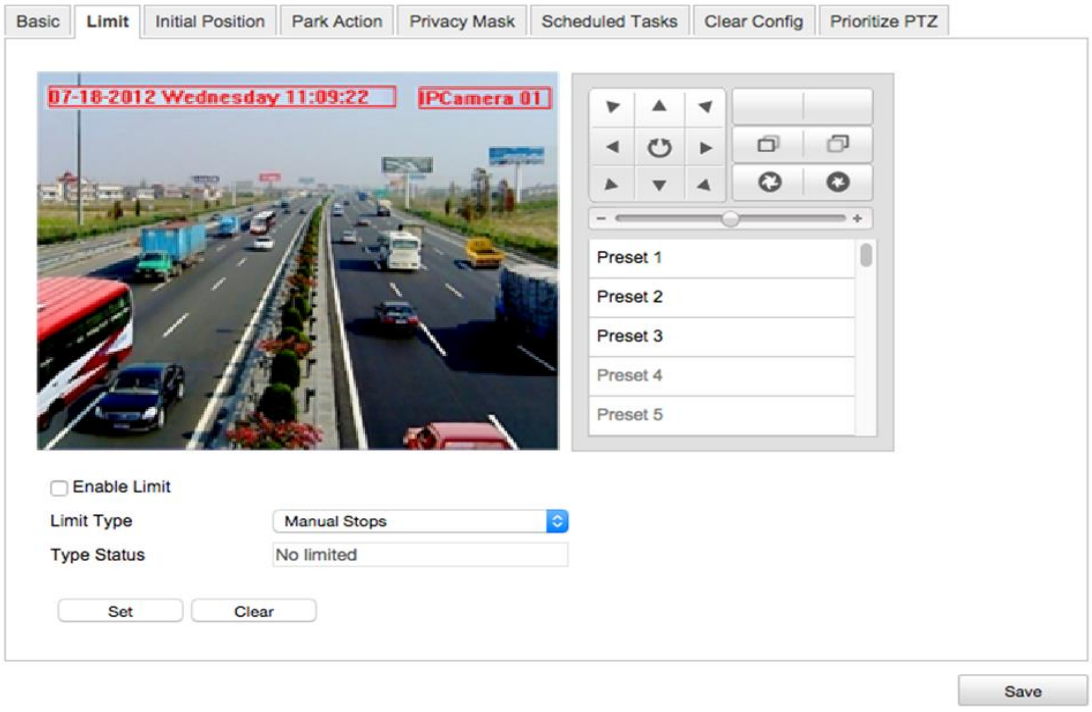
Configuring the PTZ limit settings

The Limit settings let you set a limit for camera movement.

To configure the limit settings:

1. Enter the Limit settings interface.

   Configuration > **Camera Configuration** > **PTZ** > **Limit**



2. Select the Enable Limit checkbox.

3. Select from the **Limit Type** drop-down.

   Manual Stops, movement being controlled by user.

   – or –

   Scan Stops, is automatic movement.

4. Customize the position and movement on the left. You also have the option to select a preset.
5. Click **Save**.

Configuring the initial PTZ position

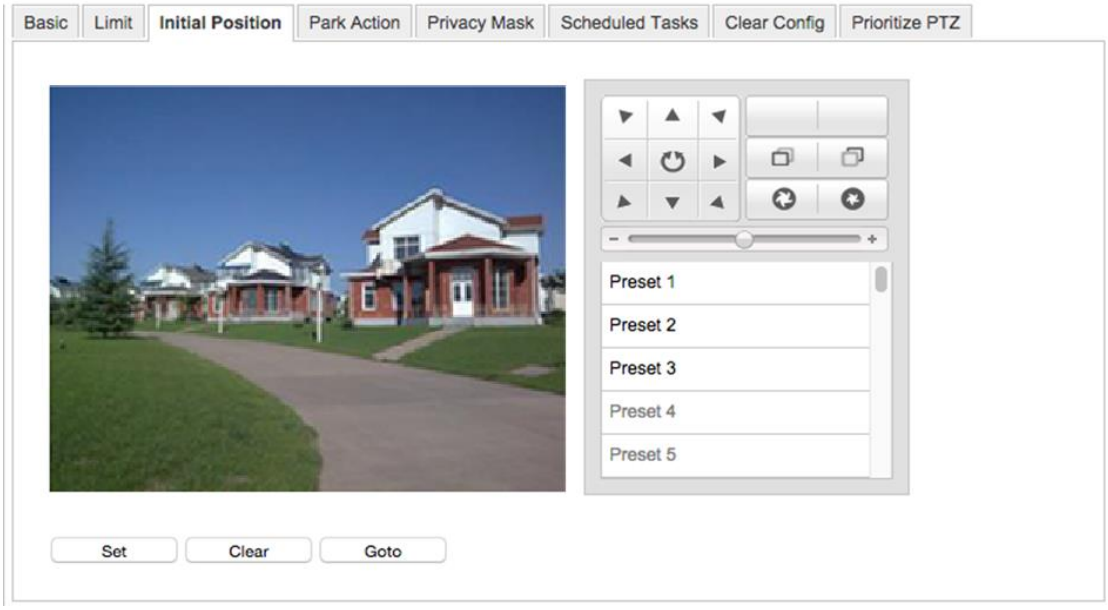
The Initial Position lets you set an initial starting position for the camera.

To configure the initial position:

1. Enter the Initial Position settings interface.

   Configuration > **Camera Configuration** > **PTZ** > **Initial Position**

2. Use the arrow, zoom, focus, iris, and touring (same controls for Live View) to set the initial position of the camera.



3. Click the **Set** button to keep the configured position settings.

   – or –

   Click the **Clear** button to clear the position settings.

   – or –

   Click **Goto** to go to the set Initial Position.

Configuring the PTZ park action

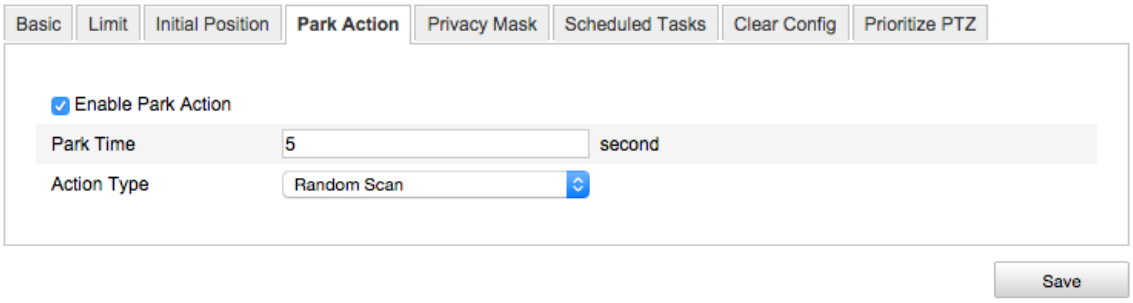
The Park Actions lets you stop the camera.

To configure the park action:

1. Enter the Park Action settings interface.

   Configuration > **Camera Configuration** > **PTZ** > **Park Action**

2. Select the Enable Park Action checkbox to enable this function.



3. In the **Park Time** field, enter a time in seconds for the park time.
4. Customize the **Action Type** drop-down from the following options.

   Auto Scan: This scans automatically.

   Frame Scan: This scans by image frame.

   Random Scan: This scans at random, stopping at random points, depending on the park action.

   Patrol: This scans in a path of presets.

   Pattern: This scans in a recorded motion sequence.

   Preset: This scans to a recorded location.

   Panorama Scan: This scans in panoramic view.

   Tilt Scan: This scans at a tilted angle, moving up and down on the Y axis.

5. Click **Save**.

Configuring the PTZ privacy mask

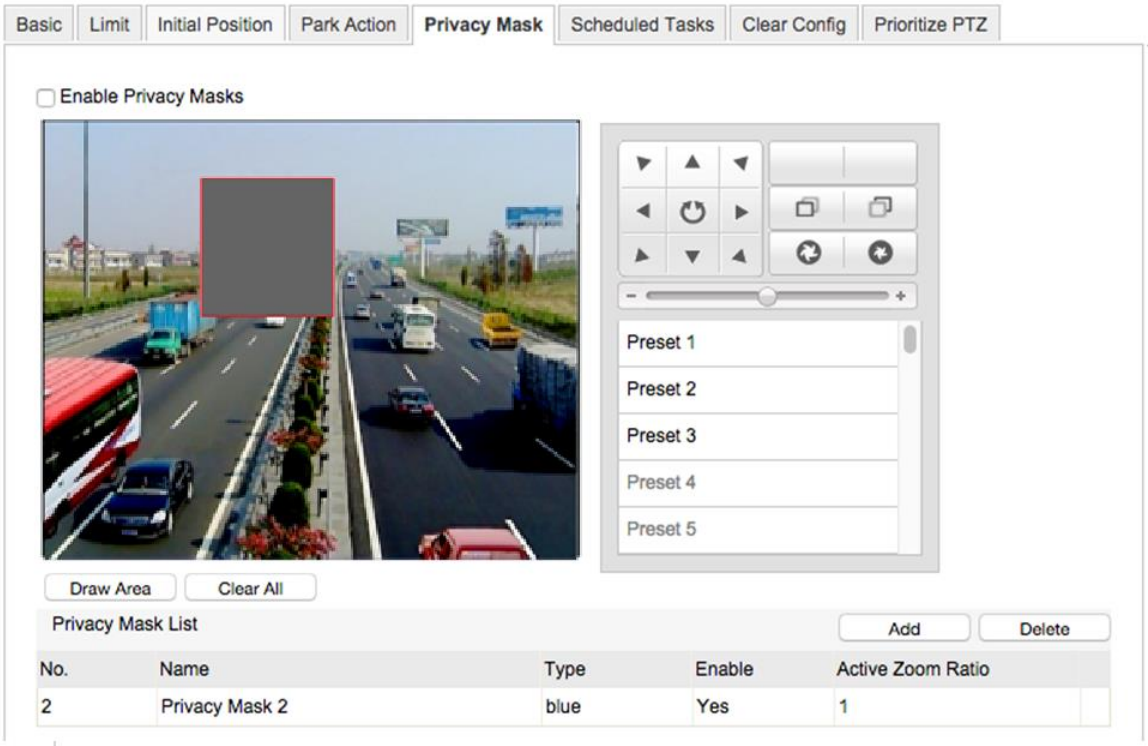
Privacy mask lets you cover certain areas on the live video to prevent zones in the surveillance area from being live viewed and recorded.

To configure privacy mask

1. Enter the Privacy Mask settings interface.

   Configuration > **Camera Configuration** > **PTZ** > **Privacy Mask**

2. Select the **Enable Privacy Mask** checkbox to enable this function.
3. Click **Draw Area**.



4. Click and drag the mouse in the live video window to draw the mask area.
5. The Privacy Mask List lets you customize the name, type, if enable, and add or delete an area.

   Note: You can set two areas on the same image.
6. Click **Stop Drawing** to finish drawing, or click **Clear All** to clear all of the areas you set without saving them.
7. Click **Save**.

Note: Privacy masks are set to a location on the view screen and are not relative to the location of the camera. The mask will stay in the same spot regardless of where the camera moves.

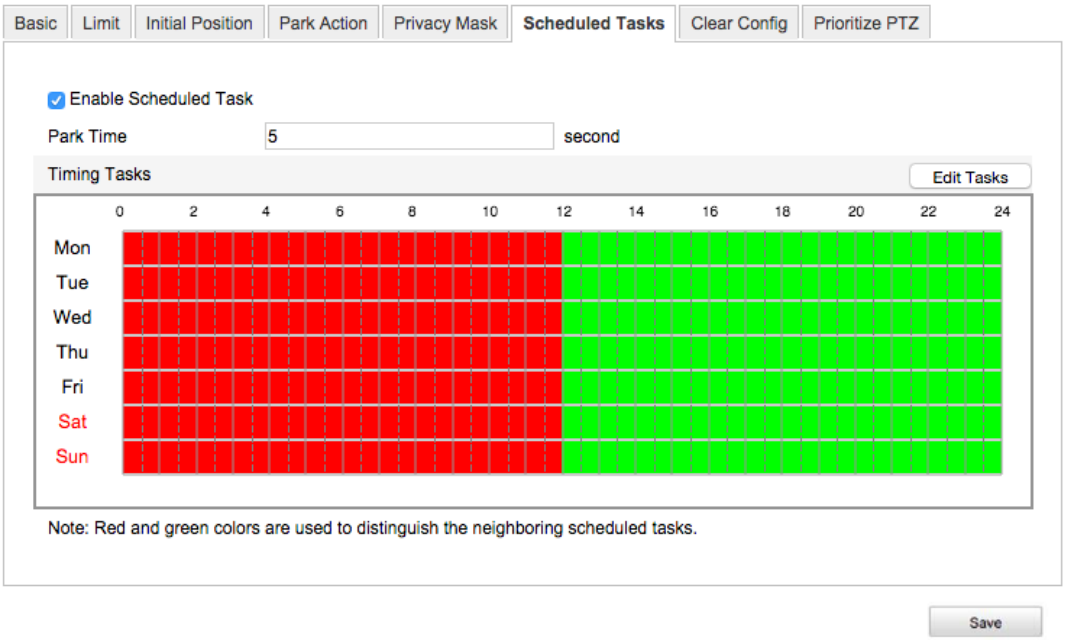
Configuring a PTZ scheduled task

Scheduled task lets you set a schedule for the PTZ tasks.

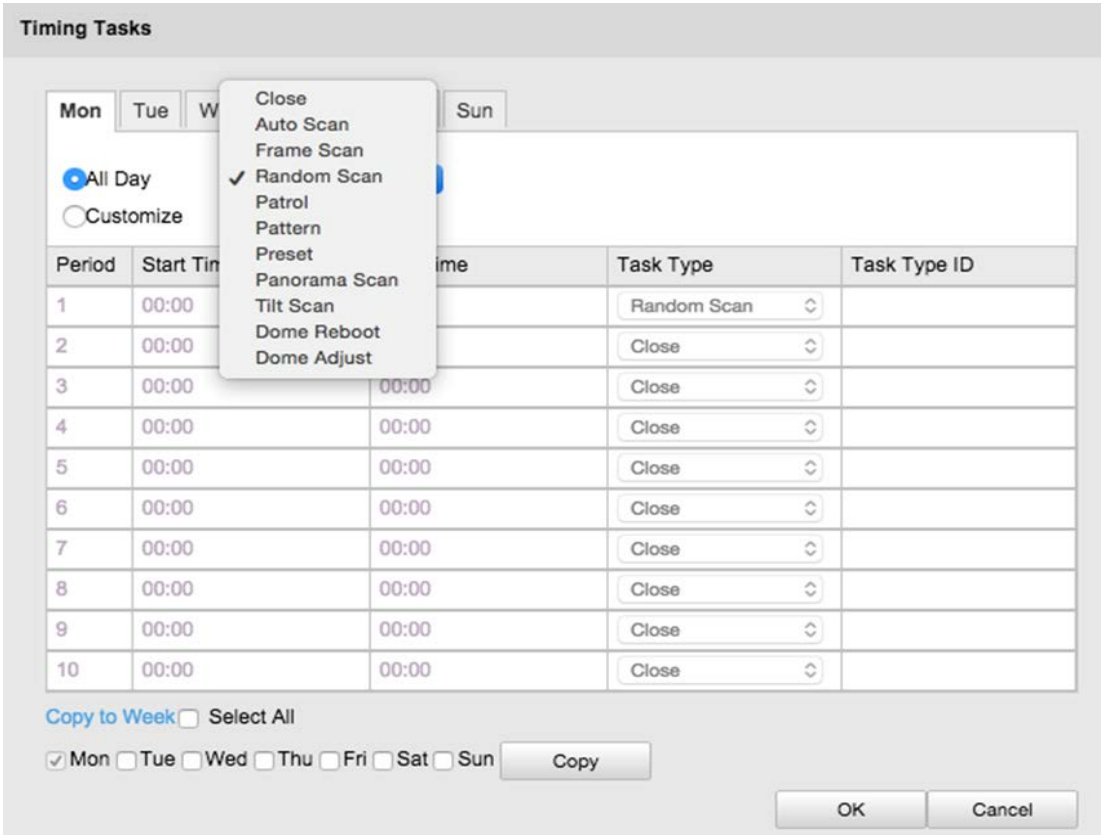
To configure a scheduled task:

1. Enter the Scheduled Task settings interface.

   Configuration > **Camera Configuration** > **PTZ** > **Scheduled Task**



2. Set a second amount in the **Park Time** field.
3. Click **Edit Tasks** to change the day, task type, start time, and end time.



Note: You can copy the tasks to other days of the week.

4. Click **Save**.

Clearing a PTZ configuration

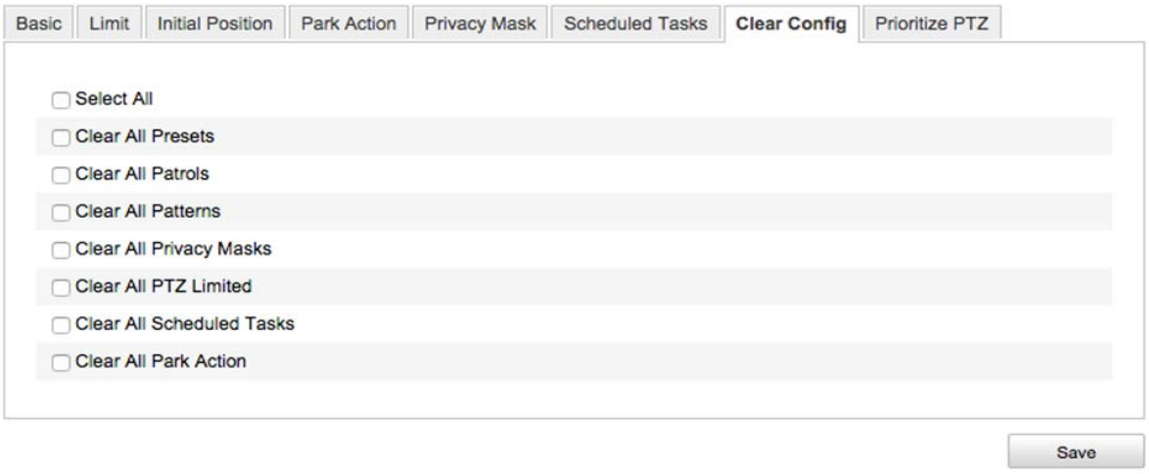
The Clear Configuration interface lets you clear other settings individually, by selection of more than one, or all at the same time.

To clear the configuration:

1. Enter the Clear Configuration settings interface.

   Configuration > **Camera Configuration** > **PTZ** > **Clear Configuration**

2. Select the checkboxes of the desired areas.



3. Click **Save**.

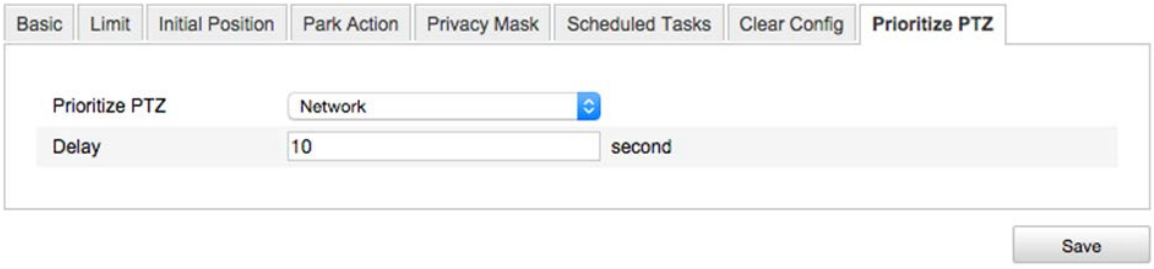
Configuring the prioritize PTZ

Prioritizing the PTZ lets you prioritize where PTZ control comes from.

To configure the prioritize PTZ:

1. Enter the Prioritize PTZ settings interface.

   Configuration > **Camera Configuration** > **PTZ** > **Prioritize PTZ**



2. In the **Prioritize PTZ** field, select Network or RS485 from the drop-down.
3. In the **Delay** field, set the time in seconds for the delay to occur.
4. Click **Save**.

Setting/calling a preset

Setting a preset allows you to switch the camera to a preset position, without having to readjust manually. The preset can be selected at any time or be set for certain events.

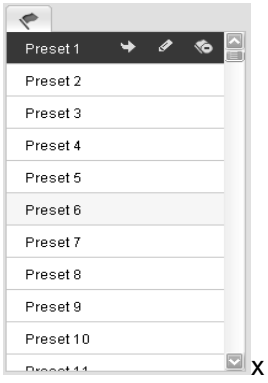
To set a Preset:

1. In the PTZ control panel, select a preset number from the list.

2. Use the PTZ control buttons to move the lens to the desired position.
   - Pan the camera to the right or left.
   - Tilt the camera up or down.
   - Zoom in or out.
   - Refocus the lens.
3. Click to finish the setting of the current preset.
4. You can click to delete the preset.

   Note: You can configure up to 128 presets.

   Calling a preset allows the camera to point to a specified preset scene manually or when an event takes place.
5. In the PTZ control panel, select a defined preset from the list and click to call the preset.



Storage settings

To configure record settings, make sure that you have a network storage device in the network, or have the SD card inserted in your camera.

Configuring NAS settings

The network disk should be available within the network and be properly configured to store the record and log files.

To add the network disk:

1. Enter the NAS (Network-Attached Storage) Settings interface.

   Configuration > **Camera Configuration** > **Storage** > **NAS**

HDD No.	Type	Server Address	File Path
1	NAS	172.6.21.99	/dvr/test01
2	NAS		
3	NAS		
4	NAS		
5	NAS		
6	NAS		
7	NAS		
8	NAS		

2. Enter the IP address of the network disk, and then enter the default file.
3. Click **Save** to add the network disk.

Note: After saving, you need to reboot the camera to activate the settings.

To initialize the added network disk:

1. Enter the HDD Settings interface.

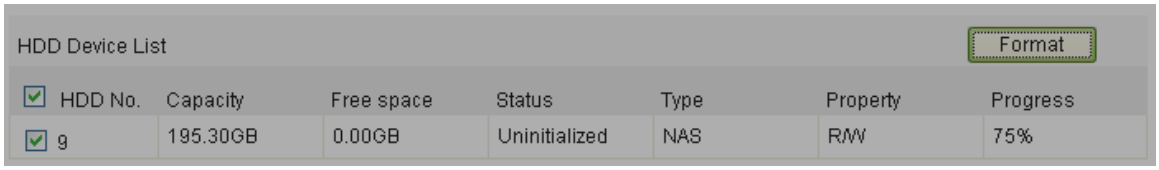
   (Camera Configuration > Storage > Storage Management)

   You can view the capacity, free space, status, type, and property of the disk in this menu.

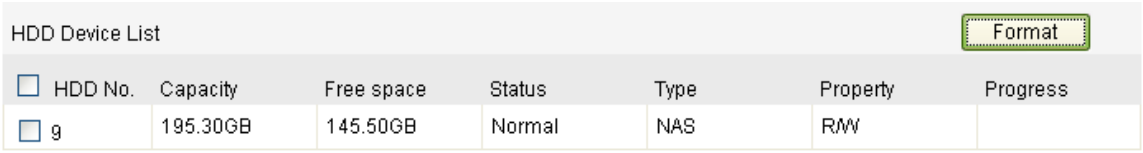
HDD Device List — Format

HDD No.	Capacity	Free space	Status	Type	Property	Progress
9	195.30GB	0.00GB	Uninitialized	NAS	R/W	

2. If the status of the disk is uninitialized, select the corresponding checkbox to select the disk, then click **Format** to start initializing the disk.



3. When initialization is completed, the status of disk will become Normal**.**



Notes

- Up to eight NAS disks can be connected to the camera.
- Refer to the NAS disk instillation to initialize and use the SD card.

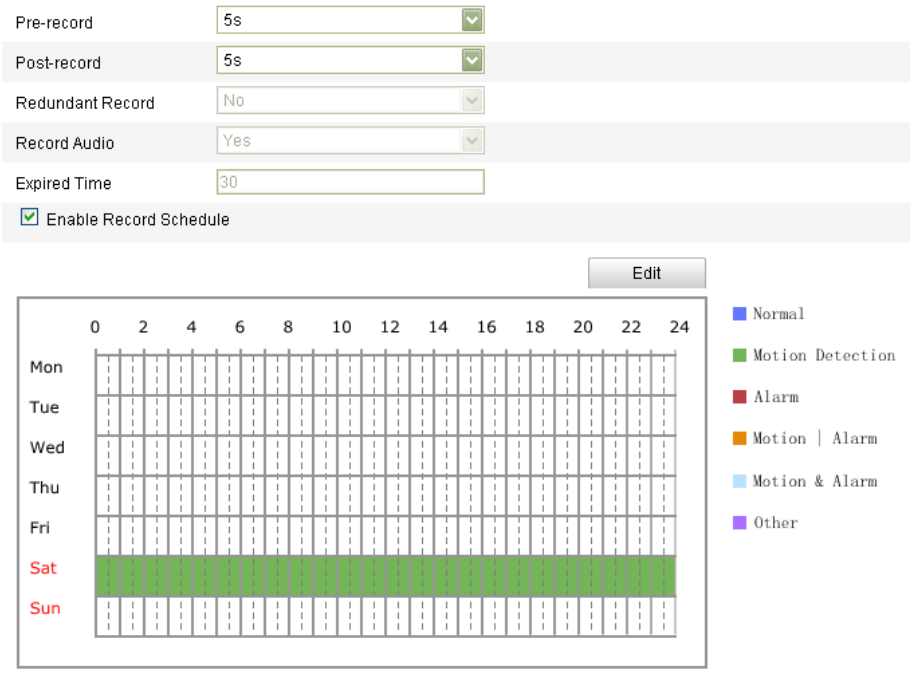
Configuring recording schedule

There are two kinds of camera recordings: manual recording and scheduled recording. In this section, you can follow the instructions to configure the scheduled recording. By default, the record files of the scheduled recording are stored in the SD card (if supported) or in the network disk.

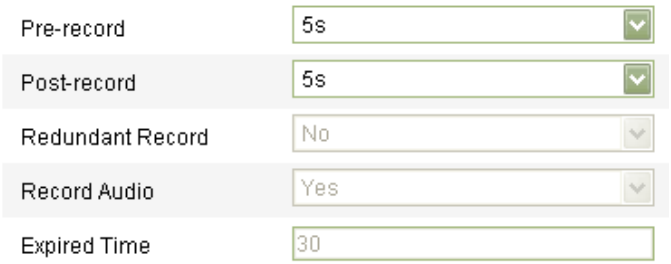
To configure a recording schedule:

1. Enter the Record Schedule Settings interface.

   Configuration > **Camera Configuration** > **Storage** > **Record Schedule**



2. Select the **Enable Record Schedule**.
3. Set the recording parameters of the camera.



Pre-record: This is the time you set to start recording before the scheduled time for the event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55.

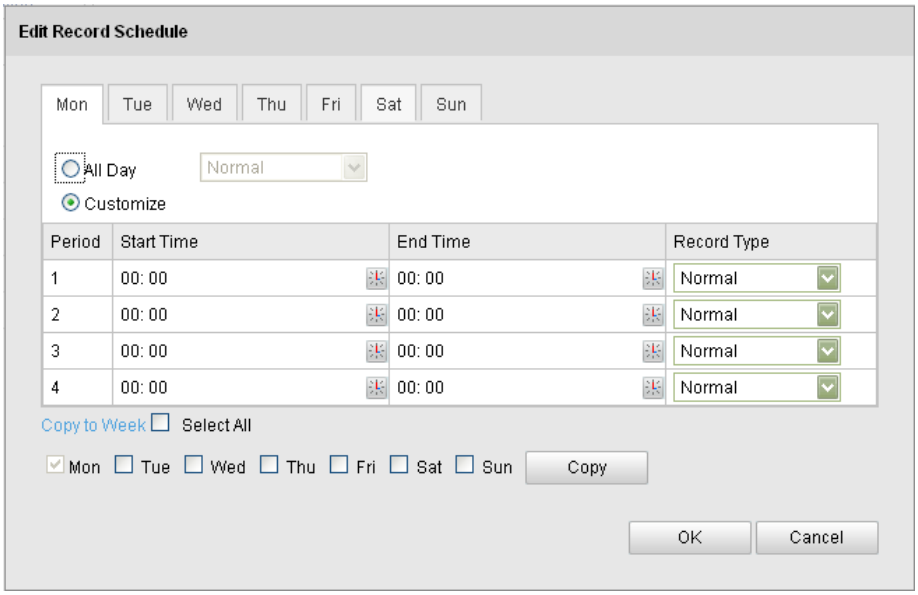
The Pre-record time can be configured as No Pre-record, 5 seconds, 10 seconds, 15 seconds, 20 seconds, 25 seconds, 30 seconds, or not limited.

Post-record: The time you set to stop recording after the scheduled time for the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.

The Post-record time can be configured as 5 seconds, 10 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes, or 10 minutes.

Note: The record parameter configurations vary depending on the camera model.

4. Click **Edit** to edit the record schedule, and then select the day to set the record schedule.



Set all-day record or segment record:

1. If you want to configure all-day recording, select the **All Day** checkbox. If you want to record in different time sections, select the **Customize** checkbox. Set the **Start Time** and **End Time.**

   Note: The time of each segment cannot be overlapped. You can configure up to four segments.

2. Select a **Record Type**. The record type can be Continuous, Motion Detection Alarm, Motion I Alarm, Motion & Alarm, PIR Alarm, Wireless Alarm, Emergency Alarm, or Manual Alarm.

   Continuous: If you select Continuous, the video will be recorded automatically according to the time of the schedule.

   Record Triggered by Motion Detection: If you select Motion Detection, the video will be recorded when the motion is detected. Configure the recording schedule, the motion detection area, and select the checkbox of Trigger Channel in the Linkage Method of the Motion Detection Settings interface.

   Record Triggered by Alarm: If you select Alarm, the video will be recorded when the alarm is triggered via the external alarm input channels. Configure the recording schedule, set the alarm type, and select the checkbox Trigger Channel in the Linkage Method of the Alarm Input Settings interface.

   Record Triggered by Motion I Alarm: If you select Motion or Alarm, the video will be recorded when the external alarm is triggered or the motion is detected. Configure the recording schedule and the settings on the Motion Detection and Alarm Input Settings interfaces.

   Record Triggered by Motion & Alarm: If you select Motion and Alarm, the video will be recorded when the motion and alarm are triggered at the same time.

Configure the recording schedule and the settings on the Motion Detection and Alarm Input Settings interfaces.

Record Triggered by PIR Alarm: If you select PIR Alarm, the video will be recorded when the PIR alarm is detected. Configure the recording schedule, set the PIR alarm, and select the checkbox of Trigger Channel in the Normal Linkage of PIR Alarm in Other Alarm Settings interface.

Record Triggered by Wireless Alarm: If you select Wireless Alarm, the video will be recorded when the wireless alarm is detected. Configure the recording schedule, set the wireless alarm, and select the checkbox of Trigger Channel in the Normal Linkage of Wireless Alarm in Other Alarm Settings interface.

Record Triggered by Emergency Alarm: If you select Emergency Alarm, the video will be recorded when the emergency alarm is detected.

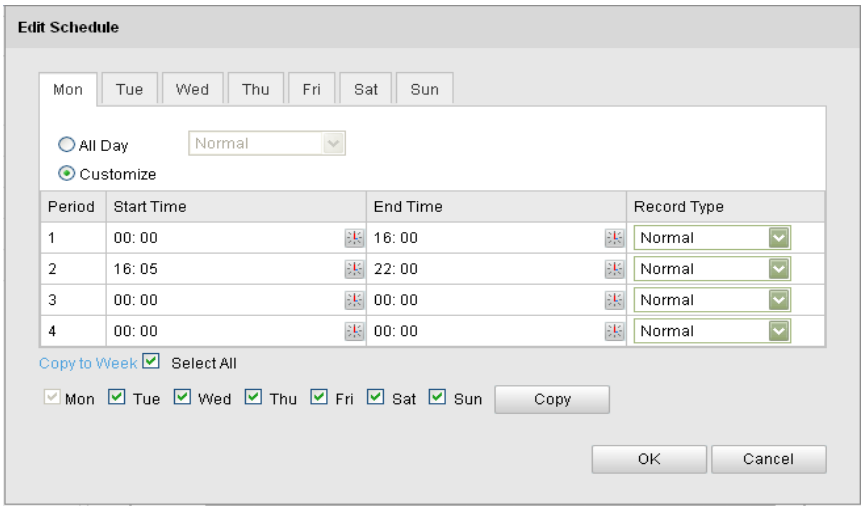
Note: This is only available for certain cameras.

Record Triggered by Manual Alarm: If you select Manual Alarm, the video will be recorded when the manual alarm is triggered.

Record Triggered by PIR, Wireless, or Manual: If you select PIR, Wireless, or Manual, the video will be recorded when the PIR alarm, the wireless alarm, or the manual alarm is detected. Configure the recording schedule and the settings for the wireless alarm and PIR alarm in the Other Alarm Settings interface.

Edit record schedule

1. Select the **Select All** checkbox, and then click **Copy** to copy settings of that day to the whole week. You can select any of the checkboxes before the date and click **Copy**.
2. Click **OK** to save the settings and exit the Edit Record Schedule interface.
3. Click **Save**.

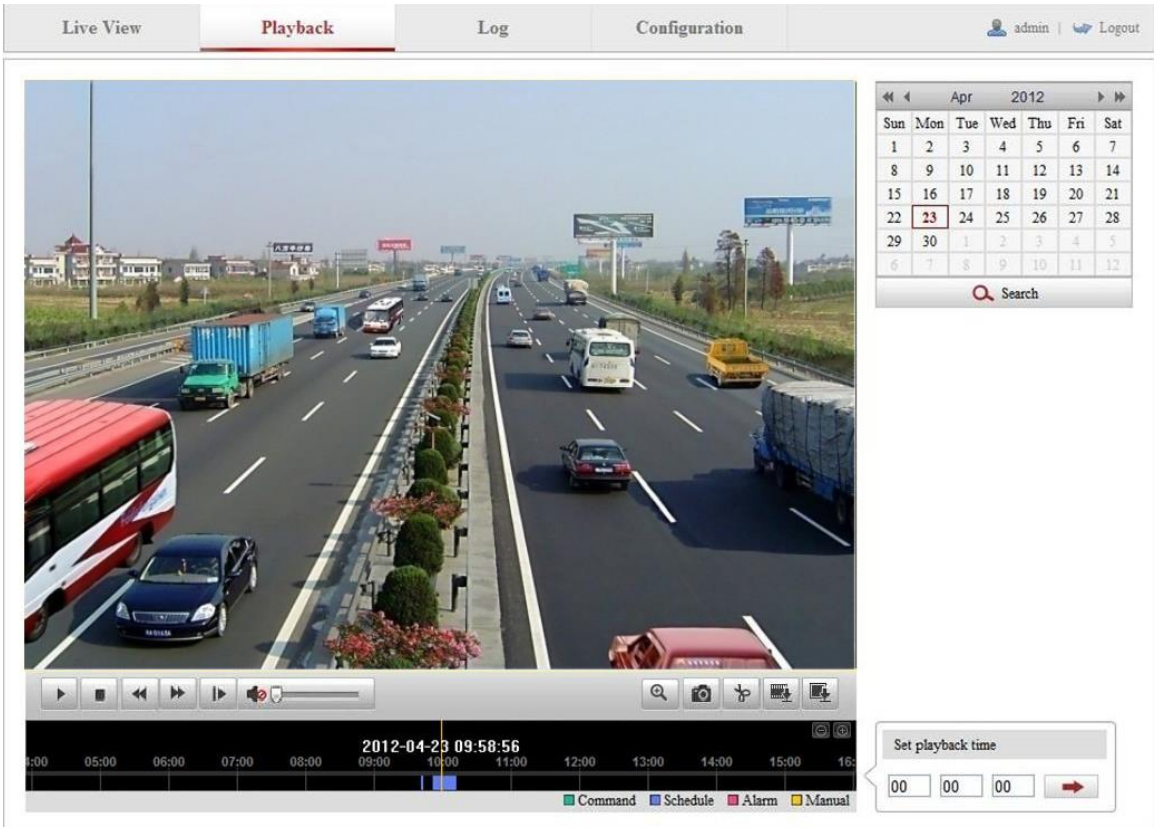


Playback

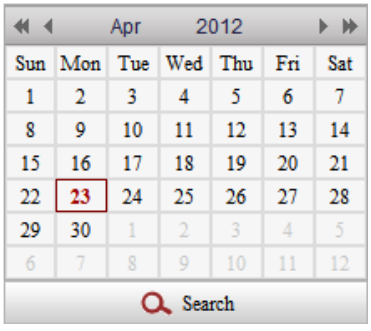
View the recorded video files stored in the network disks or SD cards.

To configure playback:

1. Click **Playback** on the menu bar to enter the playback interface.



2. Select the date and click **Search**.



3. Click to play the video files found on this date.

Use the toolbar on the bottom of Playback interface to control play.

Table 3: Description of the Playback toolbar

Icon	Operation
	Play
	Pause
	Stop
	Speed down
	Speed up
	Playback by single frame
	Capture a picture
	Start/Stop clipping video files
	Audio on and adjust volume/Mute
	Download video files
	Download captured pictures

Note: You can choose the file path locally for downloaded playback video files and pictures in Local Configuration interface.

To locate an exact playback point, you can drag the progress bar with the mouse, input the time and click , or click to zoom out/in the progress bar.

Figure 19: Set time

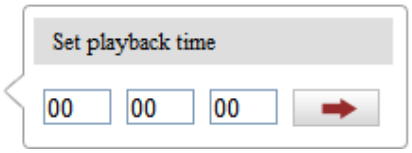
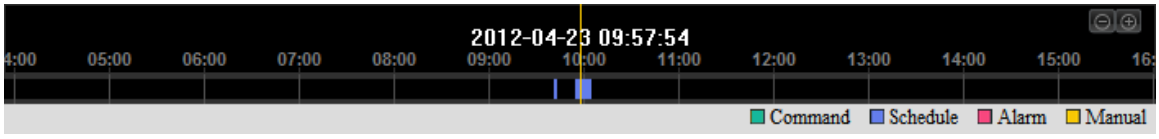


Figure 20: Progress bar



The different colors of the video on the progress bar match different video types.

Figure 21: Video type

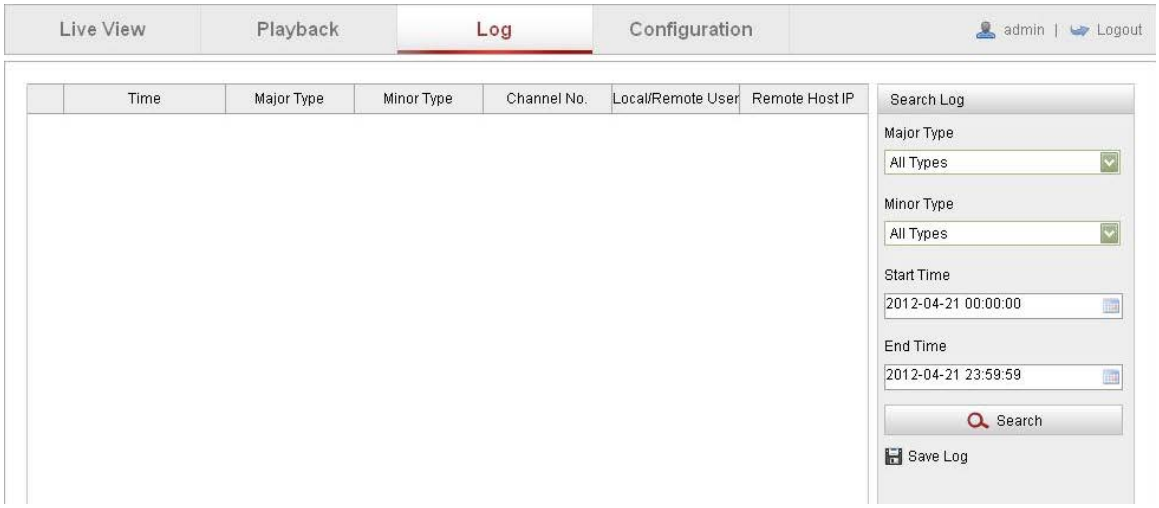
Log searching

The operation, alarm, exception, and information of the camera can be stored in log files. You can export the log files on demand.

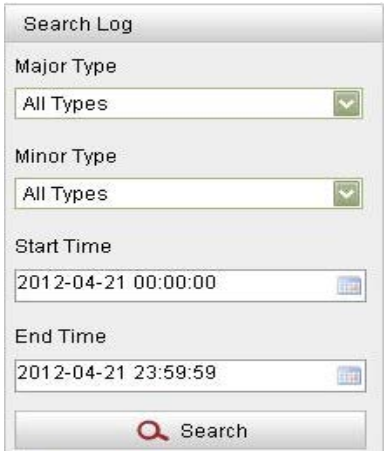
Before searching, configure the network storage for the camera, or insert an SD card in the camera.

To search logs:

1. Click **Log** on the menu bar to enter the log searching interface.



2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time, and End Time.
3. Click **Search**. The matching log files are displayed on the Log interface.



4. To export the log files, click **Save Log** and save the log files on your computer.

Others

Understanding camera capacity in an NVR

When setting up your NVR and cameras, you may notice that some of the camera images may not display in Live View. This most often occurs when you are displaying images in 1×5 mode, or 1×7 mode because the total bit rate for all cameras is exceeding the NVR's capacity. The actual capacity depends on the total bit rate from all the cameras. However, it is good practice to allow some headroom for machine operations, such as remote streaming.

NVR model	Capacity
4-channel	20 Mb
8-channel	40 Mb
16-channel	80 Mb
32-channel	160 Mb
64-channel	160 Mb

To fully understand NVR capacity, it is necessary to understand the concepts of streaming video, resolution, quality, and bit rate. Streaming video is content sent in compressed form over a network and processed in real time, that is, as it is received.

Streaming video types

Main Stream: the high quality video that is being recorded and may be streamed.

Sub Stream: never recorded; intended for streaming only. Default is 704 × 480, 584 Kbps at 8 fps.

Can be video alone, or video and audio compressed together. Audio requires very little bandwidth.

The combination of the main stream and sub streams make up the total bit rate of each camera. This is expressed in Kbps (kilobits per second) or Mbps (megabits per second).

Bit rate is determined by the selected resolution (1280 × 720, 1920 × 1080, 2560 × 1920, etc.), frame rate (frames per second), and video quality (the amount of compression being applied to each camera).

Example

32 channels of 720P cameras at 15 fps with good image quality will have 32 x (1536 + 512) = 65536 Kbps (about 66Mbps), so the 32-channel NVR can support them.

Each channel can support a different camera, as long as they do not exceed the total bit rate limit. It is entirely possible to mix 5 MP cameras with 4CIF IP cameras, etc.

Generally, 5 MP at 30 fps requires around 20 Mbps for best quality. A 4-channel NVR is currently limited to 16 Mbps.

Adjusting settings

Be aware of your NVR's capacity and make adjustments if necessary. Adjust the bit rate by lowering the resolution, frame rate, or video quality setting.

To adjust the setting:

1. Enter the Live View settings interface.
2. Adjust the Resolution, Frame Rate, and Video Quality settings.

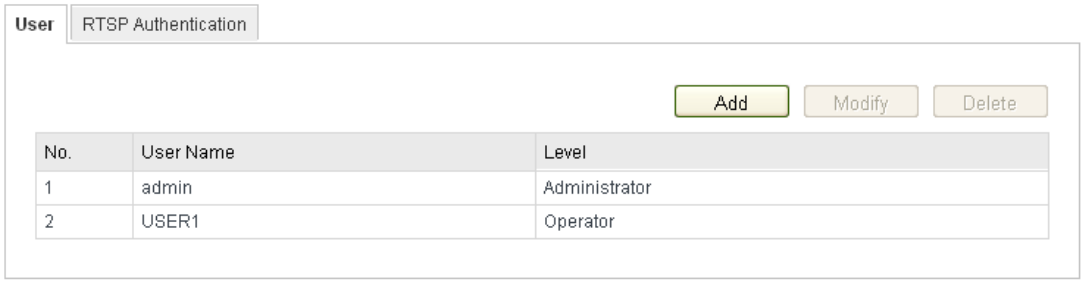
Managing user accounts

Enter the User Management interface.

Configuration > **Camera Configuration** > **Security** > **User**

Note: The admin user has access to create, modify, and delete other accounts. Up to 15 user accounts can be created.

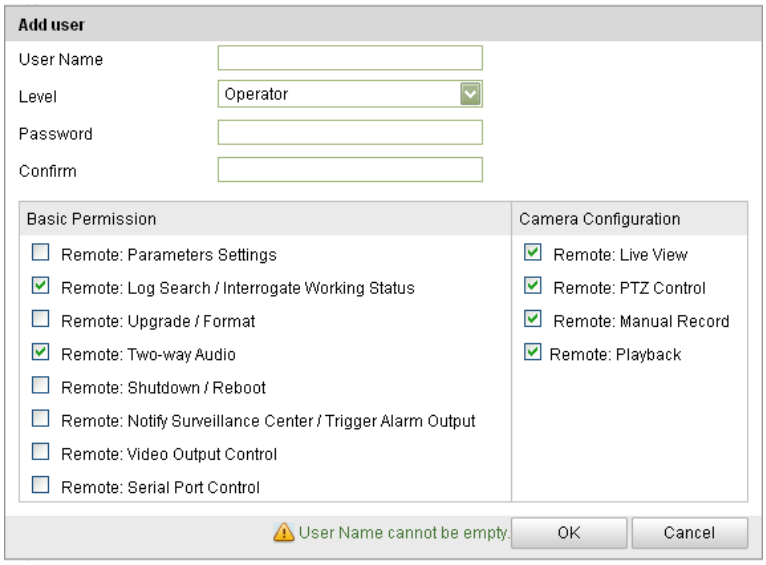
Figure 22: User interface



To add a user:

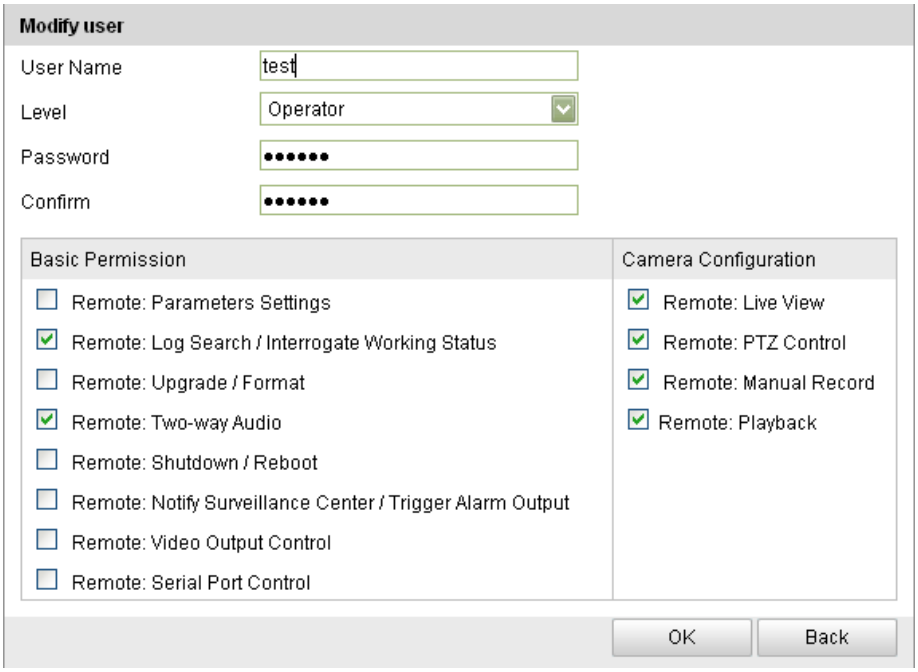
1. Click **Add** to add a user.
2. Enter the new **User Name**, select **Level,** and input **Password.**

   Note: The level indicates the permissions given to the user. You can define the user as an **Operator** or **User**.
3. In the **Basic Permission** field and **Camera Configuration** field, select or clear the permissions for the new user.
4. Click **OK** to finish the user addition.



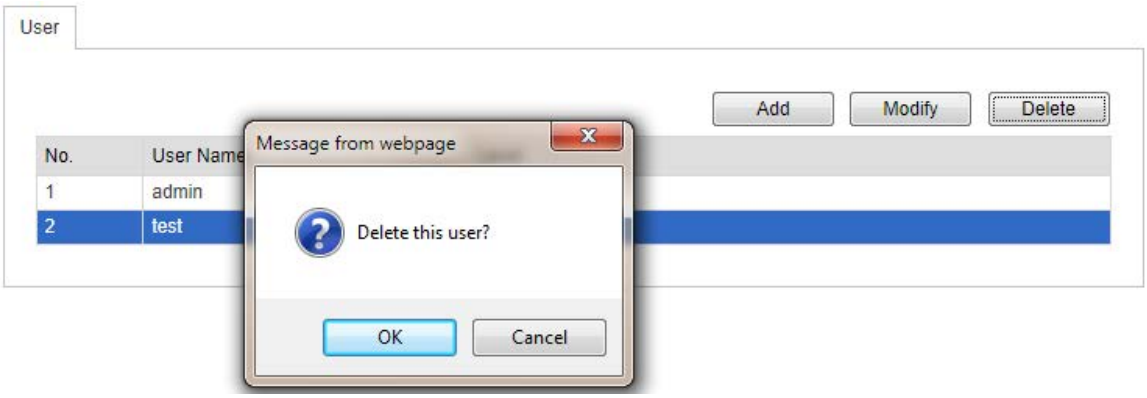
To modify a user:

1. Click to select the user from the list and click **Modify**.
2. Modify the **User Name**, **Level,** or **Password**.
3. In the **Basic Permission** field and **Camera Configuration** field, you can select or clear the permissions.
4. Click **OK** to finish the user modification.



To delete a user:

1. Click the user name you want to delete and click **Delete**.
2. Click **OK** on the pop-up dialogue box to delete the user.



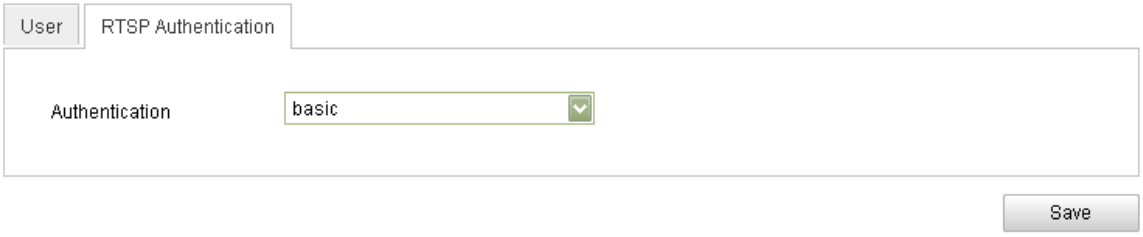
Configuring RTSP authentication

You can specifically secure the stream data of live view.

To configure RTSL authentication:

1. Enter the RTSP Authentication interface.

   Configuration > **Camera Configuration** > **Security** > **RTSP Authentication**



2. Set the Authentication type to basic or disable it in the drop-down list.

   Note: If you disable the RTSP authentication, anyone can access the video stream by the RTSP protocol using the IP address.

3. Click **Save**.

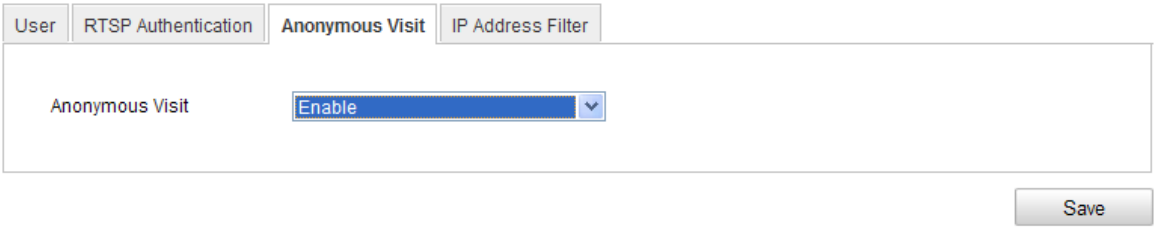
Anonymous visit

Enabling this function allows users that do not have the user name and password of the device to view it.

To set anonymous visit:

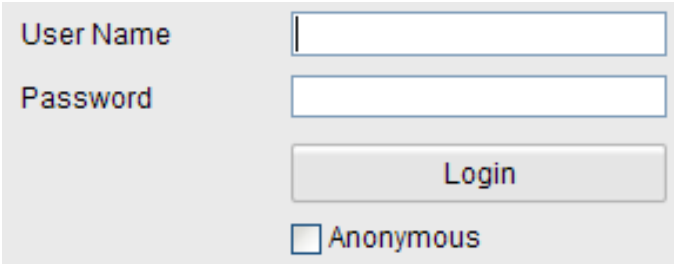
1. Enter the Anonymous Visit interface.

   Configuration > **Camera Configuration** > **Security** > **Anonymous Visit**



2. Set the Anonymous Visit permission in the drop-down list to enable or disable the anonymous visit option.
3. Click **Save**.

   The Anonymous checkbox displays the next time you log in.



4. Select the Anonymous checkbox, and then click **Login**.

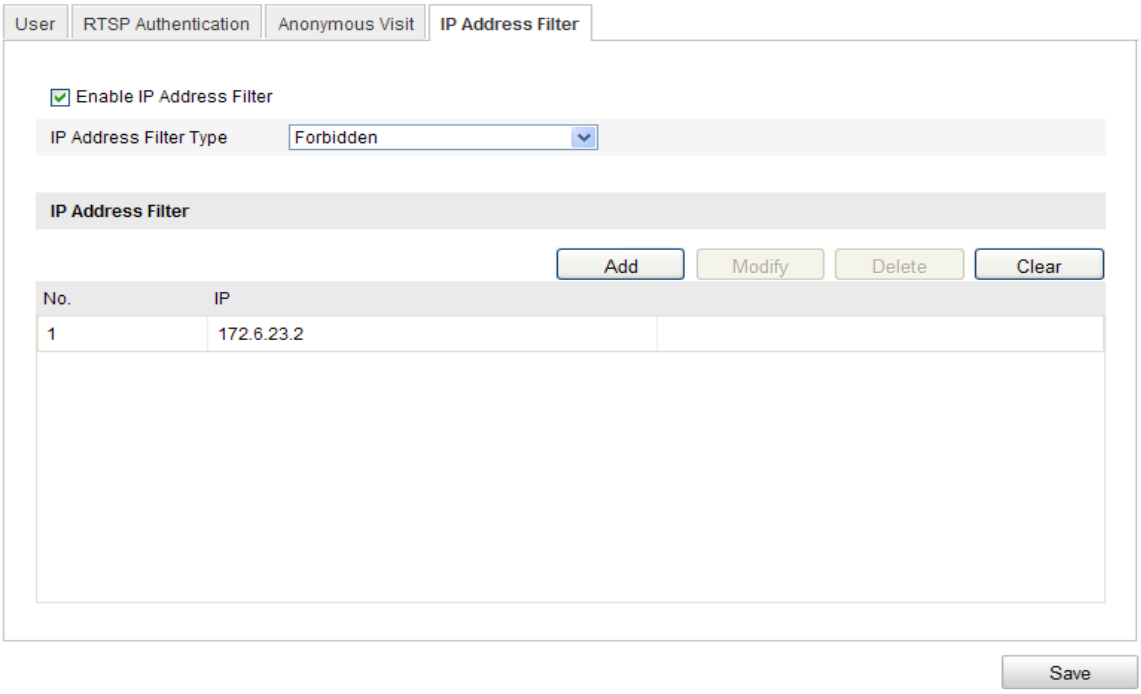
IP address filter

This function makes it possible for access control.

To configure the IP address filter:

1. Enter the IP Address Filter interface.

   Configuration > **Camera Configuration** > **Security** > **IP Address Filter**

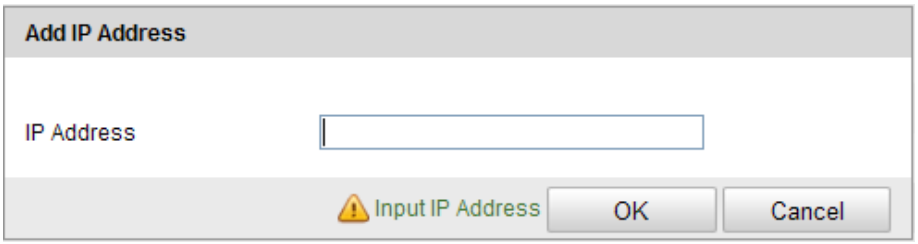


2. Select the Enable IP Address Filter checkbox.
3. Select the IP address filter from the drop-down list.

4. Select either Forbidden or Allowed.
5. Set the IP Address Filter list.

To add an IP address:

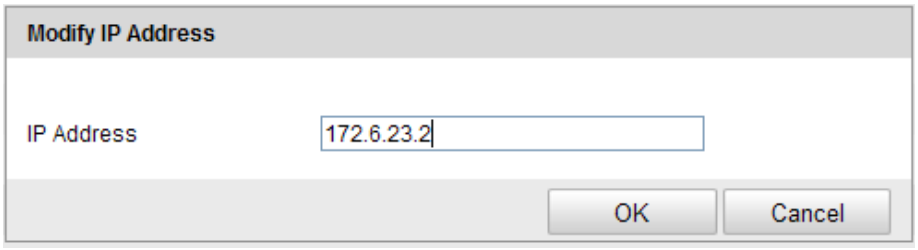
1. Click **Add** to add an IP.
2. Enter the IP Adreess.



3. Click **OK** to finish adding.

To modify an IP address:

1. Click an IP address from the filter list and click **Modify**.
2. Modify the IP address in the text filed.



3. Click **OK** to finish modifying.

To delete an IP address:

1. Click an IP address from the filter list and click **Delete**.

To delete all IP addresses:

1. Click **Clear** to delete all of the IP addrsses.
2. Click **Save**.

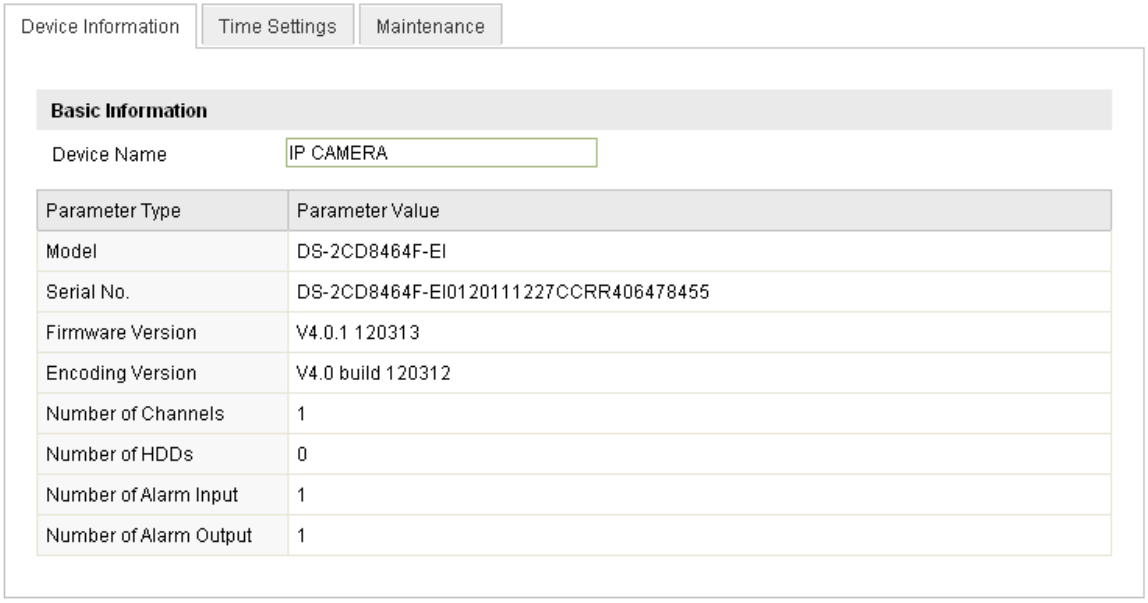
Viewing device information

Enter the Device Information interface.

Configuration > **Camera Configuration** > **System** > **Device Information**

In the Device Information interface, you can edit the device name.

Other information of the network camera, such as Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Input, and Number of Alarm Output are displayed. The information cannot be changed in this menu. It is for reference, maintenance, and modification in the future.



Maintenance

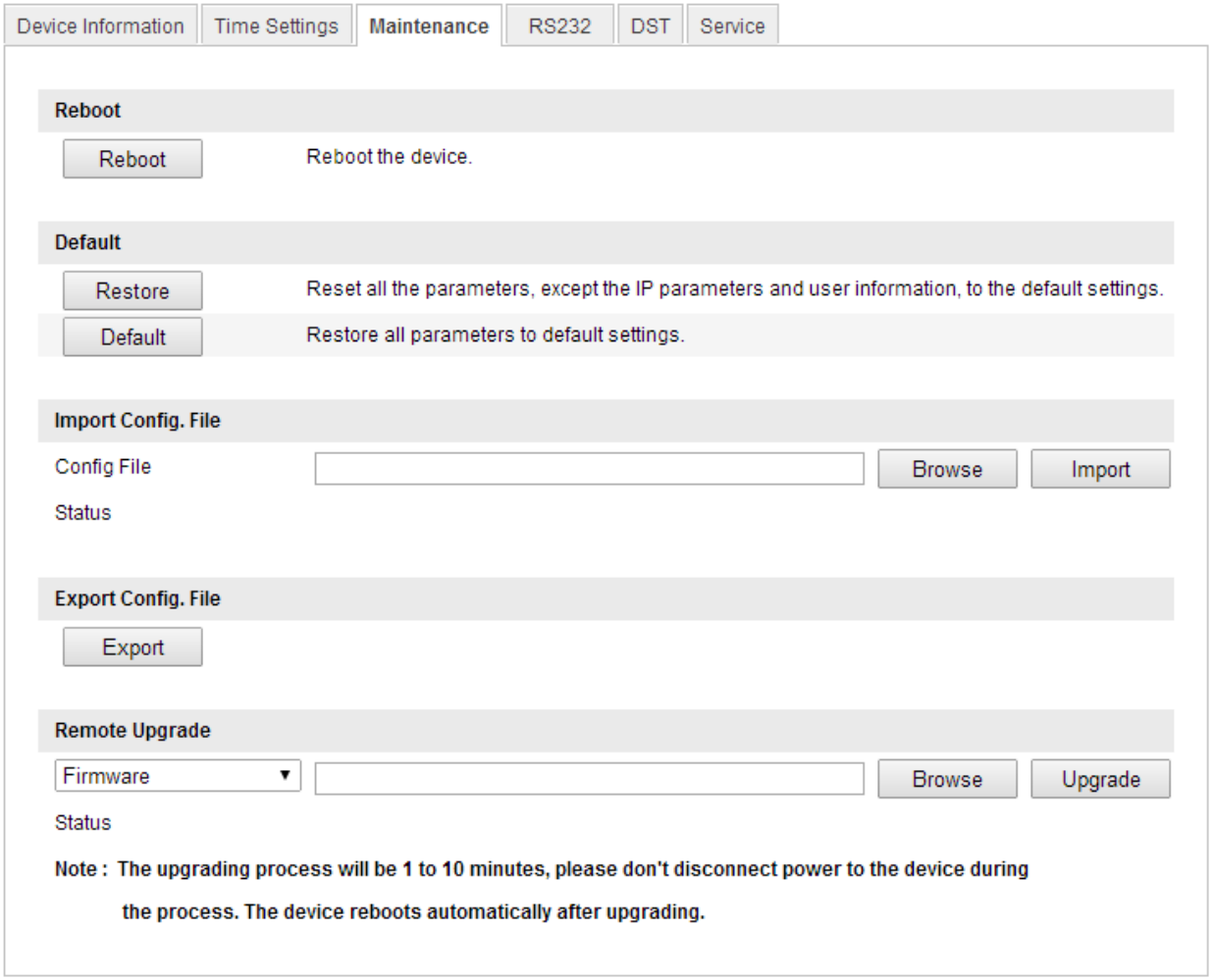
Rebooting the camera

To reboot the camera:

1. Enter the Maintenance interface.

   Configuration > **Camera Configuration** > **System** > **Maintenance**

2. Click **Reboot** to reboot the network camera.



Restoring default settings

To restore default settings:

1. Enter the Maintenance interface.

   Configuration > **Camera Configuration** > **System** > **Maintenance**

2. Click **Restore** or **Default** to restore the default settings.

Note: When restoring the default settings, the IP address returns to the default.

Importing/exporting configuration files

To import and export configuration files:

1. Enter the Maintenance interface.

   Configuration > **Camera Configuration** > **System** > **Maintenance**

2. Click **Browse** to select the local configuration file, and then click **Import** to start importing the configuration files.

   Note: You need to reboot the camera after importing a configuration file.

3. Click **Export** and set the saving path to save the configuration file in local storage**.**

Upgrading the system

To upgrade the system:

1. Enter the Maintenance interface.

   Configuration > **Camera Configuration** > **System** > **Maintenance**

2. Click **Browse** to select the local upgrade file and then click **Upgrade** to start the remote upgrade.

   Note: The upgrading process will take 1 to 10 minutes. Do not disconnect the power of the camera during this process. The camera will reboot automatically after upgrading.

RS-232 settings

The RS-232 port can be used in two ways:

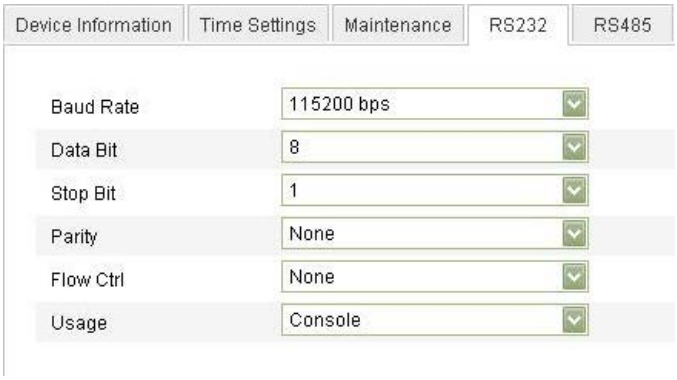
Parameters configuration: Connect a computer to the camera through the serial port. Configure the device parameters using software such as HyperTerminal. The serial port parameters must be the same as the serial port parameters of the camera.

Transparent Channel: Connect a serial device directly to the camera. The serial device will be controlled remotely by the computer through the network.

To configure RS-232 settings:

1. Enter RS-232 Port Setting interface.

   Configuration > **Camera Configuration** > **System** > **RS232**



Note: If you want to connect the camera by the RS-232 port, the parameters of the RS-232 must match the parameters configured here.

2. Click **Save**.

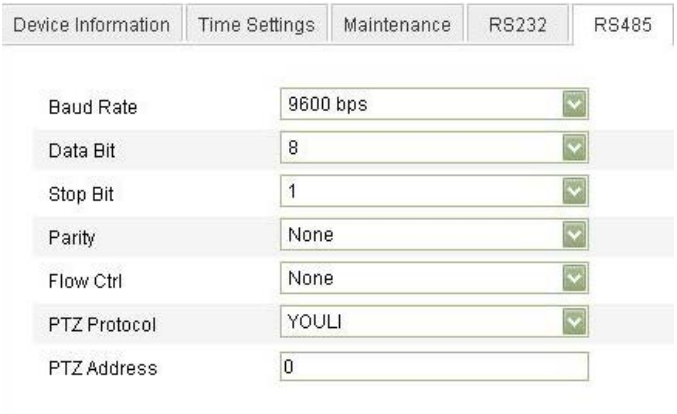
RS-485 settings

The RS-485 serial port is used to control the PTZ of the camera. Configure the PTZ parameters before you control the PTZ unit.

To configure RS-485 settings:

1. Enter RS-485 Port Setting interface.

   Configuration > **Advanced Configuration** > **System** > **RS485**



2. Set the RS-485 parameters and click **Save** to save the settings.

By default, the Baud Rate is set as 9600 bps, the Data Bit is set to 8, the stop bit is set 1, and the Parity and Flow Control is set to None.

Appendix 1

SADP software introduction

Description of SADP V 2.0

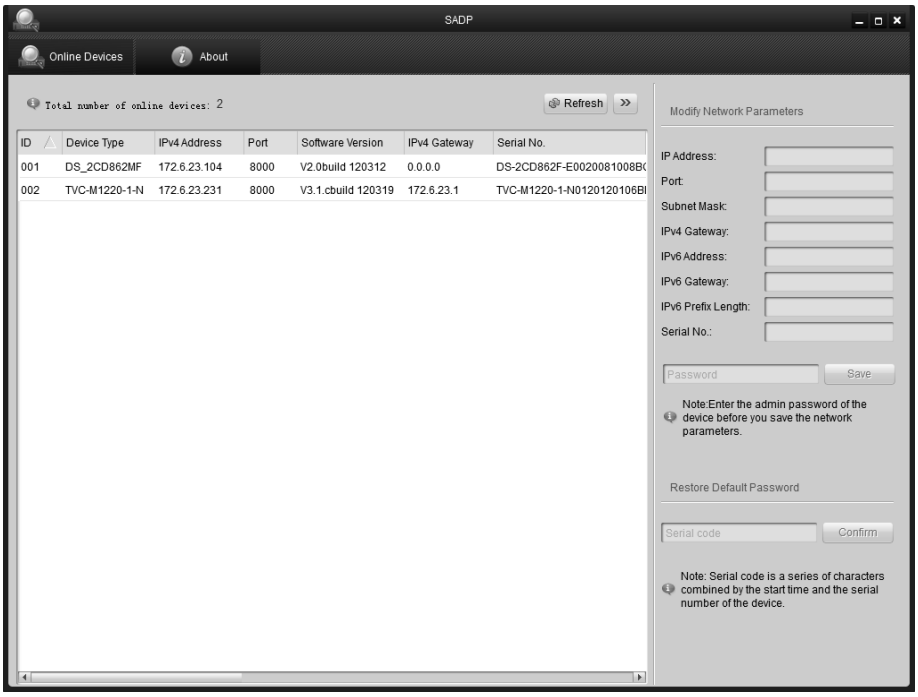
SADP (Search Active Devices Protocol) is a user-friendly, installation-free online device search tool. It searches for the active online devices in your subnet and displays their information. Using this software, you can modify the basic network information of the devices.

Note: SADP is a Windows only product.

Search active devices online

After launching the SADP software, it automatically searches for online devices every 15 seconds from your computers subnet. It displays the number and information of the searched devices in the Online Devices interface. Device information including the device type, IP address, port number, and gateway will be displayed.

Figure 23: Searching online devices



Note: Devices can be searched for and displayed in the list 15 seconds after they go online. They will be removed from the list 45 seconds after they go offline.

Search online devices manually

Click **Refresh** to refresh the online device list manually. The new devices will be added to the list.

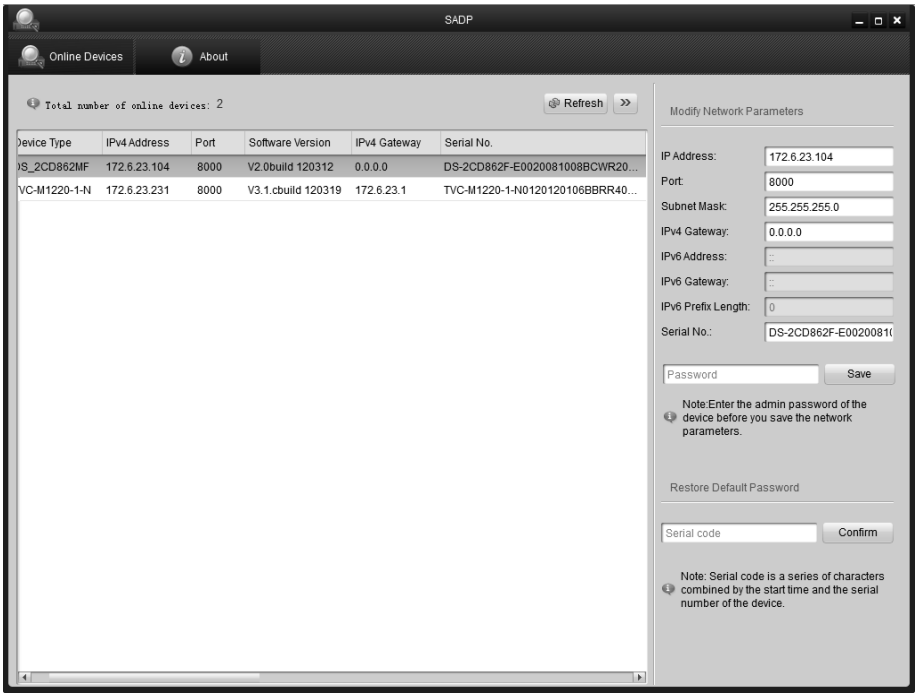
Note: You can click ▲ or ▽ on each column heading to change the order of the information.

You can click » to expand the device table and hide the network parameter panel on the right side, or click « to show the network parameter panel.

Modify network parameters

To modify network parameters:

1. Select the device to be modified in the device list and the network parameters of the device to be displayed.
2. Edit the modifiable network parameters – for example, the IP address and port number.
3. Enter the password of the admin account of the device in the Password field and click **Save**.



To restore the default password:

Enter the code in the **Serial code** field and click **Confirm** to restore the default password.

Note: The serial code is a series of characters combined by the start time and the serial number of the device.

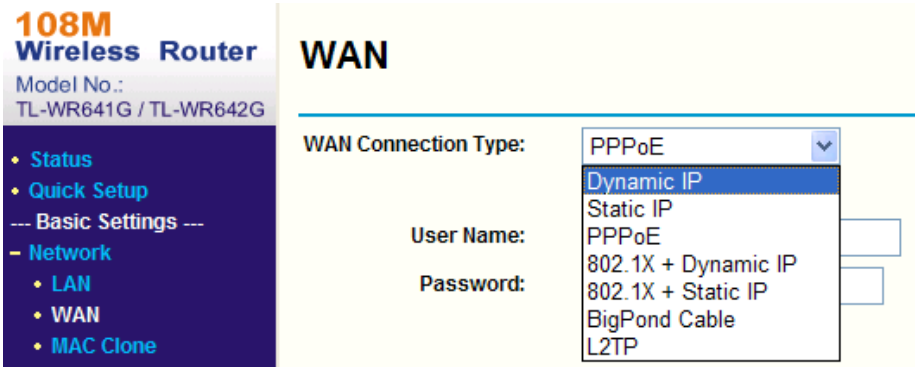
Appendix 2

Port mapping

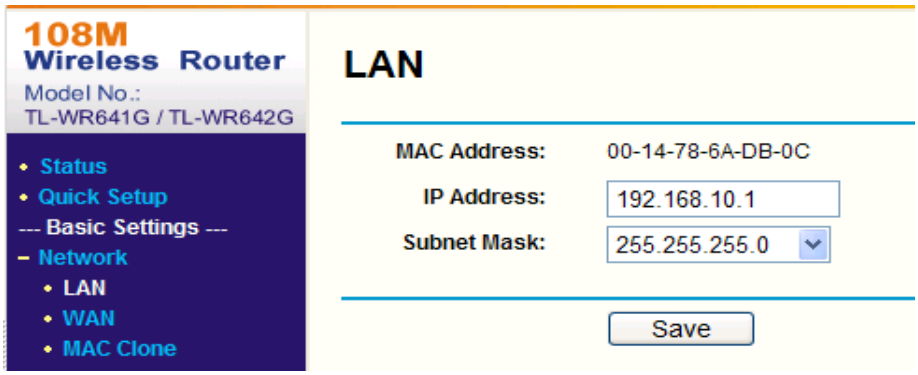
The following settings are for a TP-LINK router (TL-R410). The settings vary depending on the router model.

To set port mapping:

1. Select the WAN **Connection Type**, as shown below.



2. Set the LAN parameters of the router as in the following figure, including the IP address and subnet mask settings.



3. Set the port mapping in the virtual severs of Forwarding. By default, the camera uses port 80, 8000, 554 and 8200. You can change the port values with the web browser or the client software.

Example:

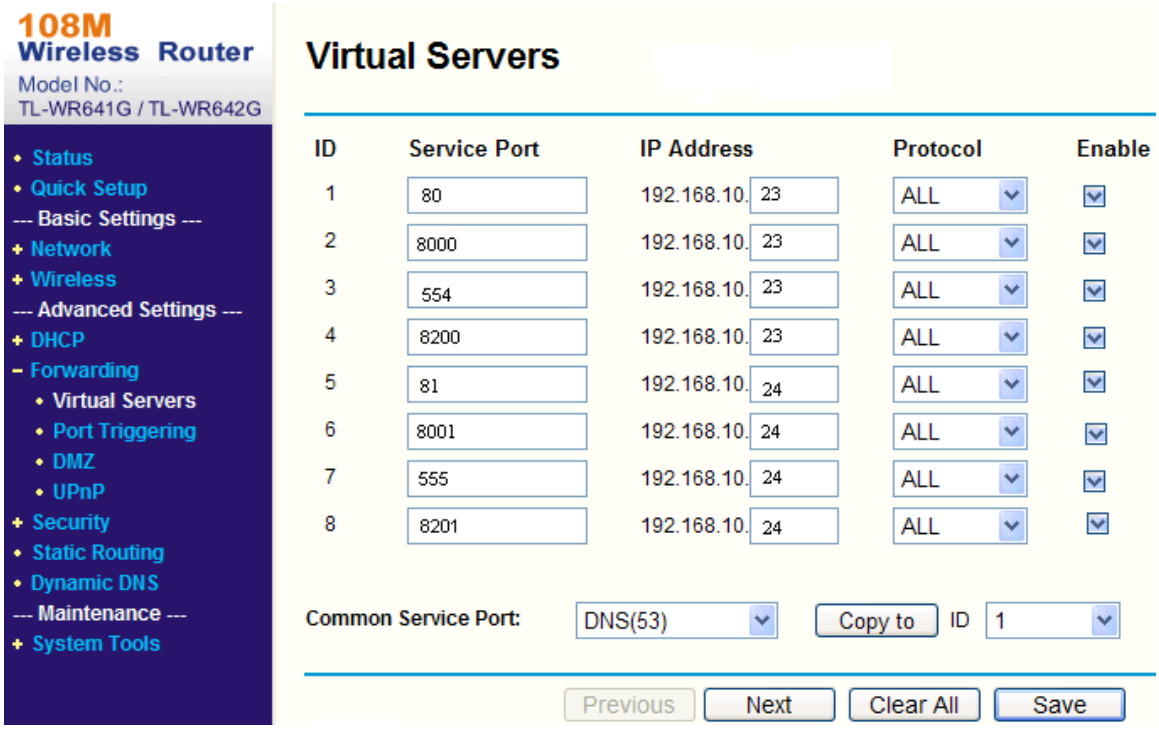
When cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, 554 and 8200 with an IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, and 8201 with an IP 192.168.1.24. Refer to the steps below:

Note: The 8200 port changes with the 8000 port with a constant value of 200. E.g. if the 8000 port is changed to 8005, then the 8200 port should be changed to 8205.

As the settings mentioned above, map the port 80, 8000, 554 and 8200 for the network camera at 192.168.1.23

To map the ports:

1. Map the port 81, 8001, 555 and 8201 for the network camera at 192.168.1.24.
2. Enable **ALL** or **TCP** protocols.
3. Select the **Enable** checkbox and click **Save**.



Note: The ports of the network camera cannot conflict with other ports. For example, the web management port of the router is 80. Change the camera port if it is the same as the management port.